

EDPB-EDPS

**Zajedničko mišljenje 4/2022
o Prijedlogu uredbe
Europskog parlamenta i
Vijeća o utvrđivanju pravila za
sprečavanje i suzbijanje
seksualnog zlostavljanja djece**

Doneseno 28. srpnja 2022.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

SADRŽAJ

1.	Kontekst	7
2.	Područje primjene mišljenja	8
3.	Opće napomene o pravima na povjerljivost komunikacija i zaštitu osobnih podataka	9
4.	Posebne napomene	12
4.1	Odnos s postojećim zakonodavstvom	12
4.1.1	Odnos s Općom uredbom o zaštiti podataka i Direktivom o e-privatnosti	12
4.1.2	Odnos s Uredbom (EU) 2021/1232 i učinak na dobrovoljno otkrivanje seksualnog zlostavljanje djece na internetu	12
4.2	Zakonita osnova na temelju Opće uredbе o zaštiti podataka	13
4.3	Obveze procjene i ublažavanja rizika	13
4.4	Uvjeti za izdavanje naloga za otkrivanje	15
4.5	Analiza nužnosti i proporcionalnosti predviđenih mjera	16
4.5.1	Djelotvornost otkrivanja	17
4.5.2	Ne postoji mjera koja manje narušava privatnost	18
4.5.3	Proporcionalnost u užem smislu	19
4.5.4	Otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece	20
4.5.5	Otkrivanje prethodno nepoznatog materijala koji sadržava seksualno zlostavljanje djece	21
4.5.6	Otkrivanje mamljenja („vrbovanja“) djece	22
4.5.7	Zaključak o nužnosti i proporcionalnosti predviđenih mjera	23
4.6	Obveze prijavljivanja	23
4.7	Obveze uklanjanja i sprečavanja pristupa	23
4.8	Relevantne tehnologije i zaštitne mjere	24
4.8.1	Tehnička i integrirana zaštita podataka	24
4.8.2	Pouzdanost tehnologija	25
4.8.3	Pregled audiokomunikacija	26
4.8.4	Provjera dobi	26
4.9	Čuvanje informacija	27
4.10	Učinak na šifriranje	27

4.11	Nadzor, provedba i suradnja	29
4.11.1	Uloga nacionalnih nadzornih tijela u skladu s Općom uredbom o zaštiti podataka	29
4.11.2	Uloga EDPB-a	29
4.11.3	Uloga EU-ova centra za seksualno zlostavljanje djece	31
4.11.4	Uloga Europolu	33
5.	Zaključak.....	36

Sažetak

Dana 11. svibnja 2022. Europska komisija predstavila je svoj Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece.

Prijedlogom bi se pružateljima usluga smještaja informacija na poslužitelju, interpersonalnih komunikacijskih usluga i drugih usluga nametnule kvalificirane obveze koje se odnose na otkrivanje, prijavljivanje, uklanjanje i sprečavanje poznatog i novog internetskog materijala koji sadržava seksualno zlostavljanje djece te mamljenje djece. Prijedlogom se predviđa i uspostava nove, decentralizirane agencije EU-a („EU-ov centar“) i mreže nacionalnih koordinacijskih tijela za pitanja seksualnog zlostavljanja djece kako bi se omogućila provedba predložene uredbe. Kako je potvrđeno u obrazloženju Prijedloga, mjere sadržane u Prijedlogu utjecale bi na ostvarivanje temeljnih prava korisnika predmetnih usluga.

Seksualno zlostavljanje posebno je teško i gnusno kazneno djelo, a cilj omogućavanja učinkovitog djelovanja u borbi protiv njega predstavlja cilj od općeg interesa koji Unija prepoznaje i kojim se nastoje zaštititi prava i slobode žrtava. Europski odbor za zaštitu podataka (EDPB) i Europski nadzornik za zaštitu podataka (EDPS) istodobno podsjećaju da sva ograničenja temeljnih prava, kao što su ona predviđena Prijedlogom, moraju biti u skladu sa zahtjevima iz članka 52. stavka 1. Povelje Europske unije o temeljnim pravima.

EDPB i EDPS ističu da Prijedlog izaziva ozbiljnu zabrinutost u pogledu proporcionalnosti predviđenog zadiranja u privatnost i ograničenja zaštite temeljnih prava na privatnost i zaštitu osobnih podataka. EDPB i EDPS u tom pogledu ističu da postupovna jamstva nikada ne mogu u potpunosti zamijeniti materijalne zaštitne mjere. Složeni sustav proširivanja razine djelovanja s procjene rizika i mjera za smanjenje rizika na nalog za otkrivanje ne može zamijeniti potrebnu jasnoću materijalnih obveza.

EDPB i EDPS smatraju da u Prijedlogu nedostaje jasnoće u pogledu ključnih elemenata, kao što su pojmovi „znatnog rizika“. Nadalje, subjekti zaduženi za primjenu tih zaštitnih mjera, počevši s privatnim subjektima pa sve do upravnih i/ili pravosudnih tijela, imaju vrlo širok prostor za slobodnu procjenu, što dovodi do pravne nesigurnosti u pogledu načina stavljanja u ravnotežu predmetnih prava u svakom pojedinom slučaju. EDPB i EDPS ističu da zakonodavac, kad dopušta posebno ozbiljno zadiranje u temeljna prava, mora osigurati pravnu jasnoću o tome kada je i gdje dopušteno zadiranje u temeljna prava. Iako priznaju da zakonodavstvo ne smije biti previše preskriptivno i mora se ostaviti određena fleksibilnost u njegovoj praktičnoj primjeni, EDPB i EDPS smatraju da je u Prijedlogu ostavljeno previše prostora za moguću zlouporabu zbog nepostojanja jasnih materijalnih normi.

Kad je riječ o nužnosti i proporcionalnosti predviđenih mjera otkrivanja, EDPB i EDPS posebno su zabrinuti zbog mjera predviđenih za otkrivanje nepoznatog materijala koji sadržava seksualno zlostavljanje djece i mamljenje djece („vrbovanje“) u interpersonalnim komunikacijskim uslugama. Zbog njihova narušavanja privatnosti, probabilističke prirode i stopa pogreške povezanih s takvim tehnologijama, EDPB i EDPS smatraju da zadiranje nastalo tim mjerama nadilazi ono što je nužno i razmjerno. Osim toga, veća je vjerojatnost da će mjere koje javnim tijelima omogućuju opći pristup sadržaju komunikacije radi otkrivanja mamljenja djece utjecati na bit prava zajamčenih člancima 7. i 8. Povelje. Stoga bi iz Prijedloga trebalo ukloniti relevantne odredbe koje se odnose na mamljenje. Osim toga, Prijedlog iz svojeg područja primjene ne isključuje pregled audiokomunikacije. EDPB i EDPS smatraju da pregled audiokomunikacije posebno narušava privatnost i da kao takav mora ostati izvan područja primjene obveza otkrivanja utvrđenih u predloženoj uredbi, i u pogledu glasovnih poruka i u pogledu komunikacije uživo.

EDPB i EDPS također izražavaju sumnje u pogledu djelotvornosti mjera za sprečavanje pristupa i smatraju da bi zahtijevanje od pružatelja internetskih usluga da dešifriraju internetsku komunikaciju kako bi se spriječio pristup komunikacijama koje se odnose na materijal koji sadržava seksualno zlostavljanje djece bilo nerazmjerno.

Nadalje, EDPB i EDPS ističu da tehnologije šifriranja bitno pridonose poštovanju privatnog života i povjerljivosti komunikacija, slobodi izražavanja te inovacijama i rastu digitalnog gospodarstva, koje se temelji na visokoj razini povjerenja i pouzdanosti koje takve tehnologije pružaju. U uvodnoj izjavi 26. Prijedloga ne navodi se samo odabir tehnologija otkrivanja, nego i tehničkih mjera za zaštitu povjerljivosti komunikacija, kao što su šifriranje, uz napomenu da taj tehnološki odabir mora ispunjavati zahtjeve predložene uredbe, tj. mora omogućiti otkrivanje. Time se podupire ideja iz članka 8. stavka 3. i članka 10. stavka 2. Prijedloga da pružatelj usluga ne može odbiti izvršenje naloga za otkrivanje na temelju tehničke nemogućnosti. EDPB i EDPS smatraju da bi trebala postojati bolja ravnoteža između društvene potrebe za sigurnim i privatnim komunikacijskim kanalima i borbe protiv njihove zlouporabe. U Prijedlogu bi trebalo jasno navesti da se ništa u predloženoj uredbi ne bi smjelo tumačiti kao zabrana ili slabljenje šifriranja.

Iako EDPB i EDPS pozdravljaju izjavu u Prijedlogu u kojoj se navodi da se ne utječe na ovlasti i na dležnosti tijela za zaštitu podataka u skladu s Općom uredbom o zaštiti podataka, EDPB i EDPS smatraju da bi odnos između zadaća koordinacijskih tijela i tijela za zaštitu podataka ipak trebalo bolje regulirati. U tom pogledu EDPB i EDPS cijene ulogu koja se Prijedlogom dodjeljuje EDPB-u, odnosno zahtjev da on sudjeluje u praktičnoj primjeni Prijedloga, posebno potrebu da EDPB daje mišljenje o tehnologijama koje bi EU-ov centar stavio na raspolaganje za izvršenje naloga za otkrivanje. Međutim, trebalo bi pojasniti koju bi svrhu mišljenje imalo u postupku i kako bi EU-ov centar postupio nakon što dobije mišljenje EDPB-a.

Naposljetku, EDPB i EDPS napominju da se Prijedlogom predviđa bliska suradnja EU-ova centra i Europolu koji bi jedan drugome trebali omogućiti „najpotpuniji pristup relevantnim informacijskim sustavima“. Iako EDPB i EDPS u načelu podupiru suradnju tih dviju agencija, s obzirom na to da EU-ov centar nije tijelo za izvršavanje zakonodavstva, EDPB i EDPS i ipak daju nekoliko preporuka za poboljšanje relevantnih odredbi, uključujući da se prijenos osobnih podataka između EU-ova centra i Europolu odvija samo na pojedinačnoj osnovi, nakon propisno ocijenjenog zahtjeva, putem alata za sigurnu razmjenu komunikacije, kao što je mreža SIENA.

Europski odbor za zaštitu podataka i Europski nadzornik za zaštitu podataka

Uzimajući u obzir članak 42. stavak 2. Uredbe (EU) 2018/1725 od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ („EUDPR”),¹

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.,²

uzimajući u obzir zahtjev Europske komisije za zajedničko mišljenje Europskog odbora za zaštitu podataka i Europskog nadzornika za zaštitu podataka od 12. svibnja 2022. o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece,³

USVOJILI SU SLJEDEĆE ZAJEDNIČKO MIŠLJENJE

1. KONTEKST

1. Dana 11. svibnja 2022. Europska komisija („Komisija”) predstavila je svoj Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece („Prijedlog” ili „predložena uredba”).⁴
2. Prijedlog je izdan nakon donošenja Uredbe (EU) 2021/1232 o privremenom odstupanju od određenih odredbi Direktive 2002/58/EZ u pogledu tehnologija koje pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga upotrebljavaju za obradu osobnih i drugih podataka u svrhu borbe protiv seksualnog zlostavljanja djece na internetu („Privremena uredba”) ⁵. Privremenom uredbom od relevantnih pružatelja usluga ne zahtijeva se uvođenje mjera za otkrivanje materijala koji sadržava seksualno zlostavljanje djece (npr. slike, videozapisi itd.) ili mamljenja djece (poznato i kao „vrbovanje”) na njihovim uslugama, ali se tim pružateljima omogućuje da to čine dobrovoljno, u skladu s uvjetima utvrđenima u toj uredbi.⁶
3. Prijedlog se sastoji od dva glavna elementa. Prvo, njime bi se pružateljima usluga smještaja informacija na poslužitelju, interpersonalnih komunikacijskih usluga i drugih usluga nametnule kvalificirane

¹ SL L 295, 21.11.2018., str. 39.

² Upućivanja na „države članice” u ovom dokumentu trebala bi se tumačiti kao upućivanja na „države članice EGP-a”.

³ Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece, COM(2022) 209 final.

⁴ Ibid.

⁵ Uredba (EU) 2021/1232 Europskog parlamenta i Vijeća od 14. srpnja 2021. o privremenom odstupanju od određenih odredbi Direktive 2002/58/EZ u pogledu tehnologija koje pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga upotrebljavaju za obradu osobnih i drugih podataka u svrhu borbe protiv seksualnog zlostavljanja djece na internetu SL [2021] L 274/41.

⁶ Vidjeti i Mišljenje 7/2020 Europskog nadzornika za zaštitu podataka o Prijedlogu privremenih odstupanja od Direktive 2022/58/EZ u svrhu suzbijanja seksualnog zlostavljanja djece na internetu (10. studenoga 2020.).

obveze koje se odnose na otkrivanje, prijavljivanje, uklanjanje i sprečavanje poznatog i novog internetskog materijala koji sadržava seksualno zlostavljanje djece te mamljenje djece. Drugo, Prijedlogom se predviđa uspostava nove, decentralizirane agencije EU-a („EU-ov centar“) i mreže nacionalnih koordinacijskih tijela za pitanja seksualnog zlostavljanja djece kako bi se omogućila provedba predložene uredbe.⁷

4. Kako je potvrđeno u obrazloženju Prijedloga, mjere sadržane u Prijedlogu utjecale bi na ostvarivanje temeljnih prava korisnika predmetnih usluga. Ta prava osobito uključuju temeljna prava na poštovanje privatnosti (uključujući povjerljivost komunikacija, kao dio šireg prava na poštovanje privatnog i obiteljskog života), zaštitu osobnih podataka te slobodu izražavanja i informiranja.⁸
5. Nadalje, takvim predloženim mjerama namjerava se nadograditi i u određenoj mjeri dopuniti postojeće zakonodavstvo EU-a o zaštiti podataka i privatnosti. U tom se pogledu u obrazloženju navodi sljedeće:

„Prijedlog se temelji na Općoj uredbi o zaštiti podataka. Pružatelji se u praksi za provedbu obrade osobnih podataka koja je potrebna za dobrovoljno otkrivanje i prijavljivanje seksualnog zlostavljanja djece na internetu pozivaju na razne osnove za obradu predviđene Općom uredbom o zaštiti podataka. Ovim se Prijedlogom utvrđuje sustav ciljanih naloga za otkrivanje i određuju se uvjeti za otkrivanje, čime se osigurava veća pravna sigurnost tih aktivnosti. Kad je riječ o obveznim aktivnostima otkrivanja koje uključuju obradu osobnih podataka, Prijedlogom i osobito nalozima za otkrivanje izdanima na temelju njega uspostavlja se osnova za takvu obradu iz članka 6. stavka 1. točke (c) Opće uredbe o zaštiti podataka, kojom se predviđa obrada osobnih podataka nužna radi poštovanja pravnih obveza voditelja obrade na temelju prava Unije ili prava države članice.

Prijedlogom su, među ostalim, obuhvaćeni pružatelji koji nude interpersonalne elektroničke komunikacijske usluge i stoga podliježu nacionalnim odredbama kojima se provodi Direktiva o e-privatnosti i njezina predložena revizija koja je trenutačno u fazi pregovora. Mjerama utvrđenima u Prijedlogu u određenoj se mjeri ograničava područje primjene prava i obveza iz relevantnih odredbi te direktive, konkretno u pogledu aktivnosti koje su nužne za izvršavanje naloga za otkrivanje. U tom pogledu Prijedlog uključuje analognu primjenu članka 15. stavka 1. te direktive.”⁹

6. S obzirom na ozbiljnost predviđenog zadiranja u temeljna prava, Prijedlog je osobito važan za zaštitu prava i sloboda pojedinaca u pogledu obrade osobnih podataka. Stoga je Komisija 12. svibnja 2022. odlučila savjetovati se s Europskim odborom za zaštitu podataka („EDPB“) i Europskim nadzornikom za zaštitu podataka („EDPS“) u skladu s člankom 42. stavkom 2. EUDPR-a.

2. PODRUČJE PRIMJENE MIŠLJENJA

7. U ovom zajedničkom mišljenju iznose se zajednička stajališta EDPB-a i EDPS-a o Prijedlogu. Mišljenje je ograničeno na aspekte Prijedloga koji se odnose na zaštitu privatnosti i osobnih podataka. U zajedničkom mišljenju posebno su istaknuta područja u kojima se Prijedlogom ne osigurava dostatna

⁷ COM(2022) 209 final, str. 17.

⁸ COM(2022) 209 final, str. 12.

⁹ COM(2022) 209 final, str. 4.–5.

zaštita temeljnih prava na privatnost i zaštitu podataka ili je potrebno daljnje usklađivanje s pravnim okvirom EU-a o zaštiti privatnosti i osobnih podataka.

8. Kako je dodatno objašnjeno u ovom zajedničkom mišljenju, Prijedlog izaziva ozbiljnu zabrinutost u pogledu nužnosti i proporcionalnosti predviđenog zadiranja i ograničenja zaštite temeljnih prava na privatnost i zaštitu osobnih podataka. Međutim, cilj ovog zajedničkog mišljenja nije pružiti iscrpan popis svih pitanja privatnosti i zaštite podataka iz Prijedloga niti dati konkretne prijedloge za poboljšanje teksta Prijedloga. Umjesto toga, u ovom zajedničkom mišljenju iznose se općenite napomene o glavnim pitanjima iz Prijedloga koje su utvrdili EDPB i EDPS. Međutim, EDPB i EDPSi dalje su na raspolaganju za davanje daljnjih napomena i preporuka suzakonodavcima tijekom zakonodavnog postupka u vezi s Prijedlogom.

3. OPĆE NAPOMENE O PRAVIMA NA POVJERLJIVOST KOMUNIKACIJA I ZAŠTITU OSOBNIH PODATAKA

9. Povjerljivost komunikacija bitan je element temeljnog prava na poštovanje privatnog i obiteljskog života, kako je utvrđeno u članku 7. Povelje Europske unije o temeljnim pravima („Povelja”).¹⁰ Osim toga, u članku 8. Povelje priznaje se temeljno pravo na zaštitu osobnih podataka. Prava na povjerljivost komunikacija i pravo na privatni i obiteljski život zajamčeni su i člankom 8. Europske konvencije o ljudskim pravima („EKLP”) i dio su ustavnih tradicija zajedničkih država članicama.¹¹
10. EDPB i EDPS podsjećaju da prava utvrđena u člancima 7. i 8. Povelje nisu apsolutna prava, već se moraju uzeti u obzir u odnosu na svoju funkciju u društvu.¹² Seksualno zlostavljanje posebno je teško i gnusno kazneno djelo, a cilj omogućavanja učinkovitog djelovanja u borbi protiv njega predstavlja cilj od općeg interesa koji Unija prepoznaje i kojim se nastoje zaštititi prava i slobode žrtava. Kad je riječ o učinkovitom djelovanju u borbi protiv kaznenih djela počinjenih protiv maloljetnika i drugih ranjivih osoba, Sud Europske unije („Sud EU-a”) istaknuo je da pozitivne obveze mogu proizlaziti iz članka 7. Povelje, kojim se od javnih tijela zahtijeva da donesu pravne mjere za zaštitu obiteljskog i privatnog života, doma i komuniciranja. Takve obveze mogu proizlaziti i iz članaka 3. i 4. Povelje u pogledu zaštite fizičkog i duševnog integriteta pojedinca i zabrane mučenja te nečovječnog i ponižavajućeg postupanja.¹³
11. Istodobno sva ograničenja prava zajamčenih Poveljom, kao što su ona predviđena Prijedlogom,¹⁴ moraju biti u skladu sa zahtjevima utvrđenima u članku 52. stavku 1. Povelje. Svaka mjera kojom se zadire u prava na povjerljivost komunikacija i pravo na privatni i obiteljski život mora prije svega

¹⁰ Vidjeti npr. Izjavu EDPB-a o reviziji Uredbe o e-privatnosti i njezinu učinku na zaštitu pojedinaca u pogledu privatnosti i povjerljivosti njihovih komunikacija (25. svibnja 2018.).

¹¹ Gotovo svi europski ustavi uključuju pravo na zaštitu povjerljivosti komunikacija. Viđjeti npr. članak 15. Ustava Talijanske Republike; članak 10. Temeljnog zakona Savezne Republike Njemačke; članak 42. belgijskog Ustava; i članak 13. Ustava Kraljevine Nizozemske.

¹² Vidjeti, među ostalim, presudu Suda EU-a, predmet *Facebook Ireland i Schrems*, t. 172. i u njoj navedenu sudsku praksu. Viđjeti i uvodnu izjavu 4. Opće uredbe o zaštiti podataka.

¹³ Sud EU-a, spojeni predmeti C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i dr.*, točke 126.-128. Viđjeti i Mišljenje 7/2020 Europskog nadzornika za zaštitu podataka o Prijedlogu privremenih odstupanja od Direktive 2022/58/EZ u svrhu suzbijanja seksualnog zlostavljanja djece na internetu (10. studenoga 2020.), t. 12.

¹⁴ Usp. COM(2022) 209 final, str. 12.-13.

poštovati bit prava o kojima je riječ.¹⁵ Bit prava dovodi se u pitanje ako je pravo lišeno svojeg osnovnog sadržaja i ako ga pojedinac ne može ostvariti¹⁶. Zadiranje ne može predstavljati, u odnosu na cilj koji se nastoji postići, takvo neproporcionalno i neprihvatljivo zadiranje kojim se ugrožava sama bit takvog zajamčenog prava.¹⁷ To znači da čak i temeljno pravo koje nije apsolutno, kao što su pravo na povjerljivost komunikacija i pravo na zaštitu osobnih podataka, ima neke ključne elemente koji se ne mogu ograničiti.

12. Sud EU-a u nekoliko je navrata primijenio test „bitnog sadržaja prava“ u području privatnosti elektroničkih komunikacija. U predmetu *Tele2 Sverige i Watson* Sud je donio odluku da propis kojim se ne dopušta zadržavanje sadržaja komunikacije ne može negativno utjecati na bitan sadržaj prava na privatni život i zaštitu osobnih podataka.¹⁸ U predmetu *Schrems* Sud je utvrdio da propis koji javnim tijelima omogućuje općenit pristup sadržaju elektroničkih komunikacija povređuje bitan sadržaj temeljnog prava na poštovanje privatnog života koje je zajamčeno u članku 7. Povelje.¹⁹ U predmetu *Digital Rights Ireland i Seitlinger i dr.* Sud je utvrdio da iako zadržavanje podataka koje se zahtijeva Direktivom 2006/24 predstavlja osobito teško miješanje u temeljno pravo na privatnost i druga prava utvrđena u članku 7. Povelje, ono nije takve naravi da bi povrijedilo navedeni sadržaj s obzirom na to da ta direktiva ne dopušta uvid u sadržaj elektroničke komunikacije kao takav.²⁰ Iz te se sudske prakse može zaključiti da je vjerojatnije da će mjere kojima se javnim tijelima omogućuje opći pristup sadržaju komunikacije utjecati na bit prava zajamčenih člancima 7. i 8. Povelje. Ta su razmatranja jednako relevantna i u pogledu mjera za otkrivanje materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece, poput onih predviđenih Prijedlogom.
13. Nadalje, Sud EU-a utvrdio je da mjere za sigurnost podataka imaju ključnu ulogu u osiguravanju toga da se ne povrijedi bit temeljnog prava na zaštitu osobnih podataka iz članka 8. Povelje.²¹ U digitalnom dobu tehnička rješenja za osiguravanje i zaštitu povjerljivosti elektroničkih komunikacija, uključujući mjere za šifriranje, ključna su za osiguravanje uživanja svih temeljnih prava.²² Tome bi se trebalo pridati pozornost pri procjeni mjera za obvezno otkrivanje materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece, posebno ako bi one dovele do slabljenja šifriranja.²³
14. Članak 52. stavak 1. Povelje također predviđa da sva ograničenja pri ostvarivanju temeljnog prava zajamčenog Poveljom moraju biti predviđena zakonom. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.²⁴ Kako bi se ispunio zahtjev

¹⁵ Članak 52. stavak 1. Povelje.

¹⁶ Vidjeti Smjernice Europskog nadzornika za zaštitu podataka o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka (19. prosinca 2019.), str. 8., dostupne na adresi: https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

¹⁷ Sud EU-a, predmet C-393/19, *OM*, t. 53.

¹⁸ Sud EU-a, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige i Watson*, t. 101.

¹⁹ Sud EU-a, predmet C-362/14, *Schrems*, t. 94.

²⁰ Sud EU-a, spojeni predmeti C-293/12 i C-594/12 *Digital Rights Ireland i Seitlinger i dr.*, t. 39.

²¹ *Ibid.*, t. 40.

²² Vidjeti Rezoluciju 47/16 Vijeća za ljudska prava o promicanju, zaštiti i uživanju ljudskih prava na internetu, dokument UN-a A/HRC/RES/47/16 (26. srpnja 2021.).

²³ Vidjeti također uvodnu izjavu 25. Privremene uredbe.

²⁴ Vidjeti „Procjena nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka: skup alata“, 11. travnja 2019., dostupno na https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

proporcionalnosti, zakonodavstvom se moraju utvrditi jasna i precizna pravila kojima se uređuju područje primjene i primjena predmetnih mjera te propisati minimalne zaštitne mjere kako bi osobe čiji su osobni podatci ugroženi imale dovoljna jamstva da će podatci biti učinkovito zaštićeni od rizika od zlouporabe.²⁵ U tom se propisu mora navesti i to u kojim se okolnostima i pod kojim uvjetima može donijeti mjera kojom se predviđa obrada takvih podataka, čime se osigurava da zadiranje bude ograničeno na ono što je strogo nužno.²⁶ Kako je pojasnio Sud EU-a, potreba za tim zaštitnim mjerama tim je veća kada se osobni podatci podvrgavaju automatskoj obradi i kada je u pitanju zaštita određene kategorije osobnih podataka koji su osjetljivi podatci.²⁷

15. Prijedlogom bi se ograničilo ostvarivanja prava i obveza predviđenih člankom 5. stavcima 1. i 3. te člankom 6. stavkom 1. Direktive 2002/58/EZC („Direktiva o e-privatnosti”)²⁸ u mjeri u kojoj je to potrebno za izvršavanje naloga za otkrivanje izdanih u skladu s odjeljkom 2. Poglavlja 1. Prijedloga. Stoga EDPB i EDPS smatraju da je nužno ocijeniti Prijedlog ne samo s obzirom na Povelju i Opću uredbu o zaštiti podataka, nego i s obzirom na članke 5., 6. i 15. stavak 1. Direktive o e-privatnosti.

²⁵ Sud EU-a, spojeni predmeti C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i dr.*, t. 132.

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), kako je izmijenjena Direktivom 2006/24/EZ i Direktivom 2009/136/EZ.

4. POSEBNE NAPOMENE

4.1 Odnos s postojećim zakonodavstvom

4.1.1 Odnos s Općom uredbom o zaštiti podataka i Direktivom o e-privatnosti

16. U Prijedlogu se navodi da se njime ne dovode u pitanje pravila koja proizlaze iz drugih akata Unije, posebno Opće uredbe o zaštiti podataka²⁹ i Direktive o e-privatnosti. Za razliku od Privremene uredbe, Prijedlogom se ne predviđa izričito privremeno odstupanje, nego ograničenje ostvarivanja prava i obveza utvrđenih u članku 5. stavcima 1. i 3. i članku 6. stavku 1. Direktive o e-privatnosti. Nadalje, treba napomenuti da se u Privremenoj uredbi predviđa odstupanje isključivo od odredaba članka 5. stavka 1. i članka 6. stavka 1., a ne od članka 5. stavka 3. Direktive o e-privatnosti.
17. U Prijedlogu se dalje upućuje na članak 15. stavak 1. Direktive o e-privatnosti kojim se državama članicama dopušta donošenje zakonodavnih mjera za ograničavanje područja primjene prava i obveza iz članka 5. i 6. te Direktive kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru u demokratskom društvu, među ostalim, radi sprečavanja, istrage, otkrivanja i progona kaznenih djela. Na temelju Prijedloga, članak 15. stavak 1. Direktive o e-privatnosti po analogiji se primjenjuje kada se Prijedlogom ograničava ostvarivanja prava i obveza iz članka 5. stavaka 1. i 3. te članka 6. stavka 1. Direktive o e-privatnosti.
18. EDPB i EDPS podsjećaju da je Sud EU-a jasno naveo da članak 15. stavak 1. Direktive o e-privatnosti treba usko tumačiti, što znači da iznimka od načela povjerljivosti komunikacija, koja se dopušta člankom 15. stavkom 1., mora ostati iznimka i ne smije postati pravilo.³⁰ Kako je dalje navedeno u ovom zajedničkom mišljenju, EDPB i EDPS smatraju da Prijedlog ne ispunjava zahtjeve u pogledu (stroge) nužnosti, djelotvornosti i proporcionalnosti. Nadalje, EDPB i EDPS zaključuju da bi Prijedlog podrazumijevao da zadiranje u privatnost komunikacija zapravo može postati pravilo, a ne ostati iznimka.

4.1.2 Odnos s Uredbom (EU) 2021/1232 i učinak na dobrovoljno otkrivanje seksualnog zlostavljanje djece na internetu

19. U skladu s člankom 88. Prijedloga, njime bi se stavila izvan snage Privremena uredba, kojom se predviđa privremeno odstupanje od određenih odredaba Direktive o e-privatnosti kako bi se pružateljima brojevno neovisnih interpersonalnih komunikacijskih usluga omogućila dobrovoljna upotreba tehnologija za otkrivanje materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece. Stoga od datuma početka primjene predložene uredbe ne bi postojala odstupanja od Direktive o e-privatnosti kojima bi se tim pružateljima omogućilo dobrovoljno otkrivanje seksualnog zlostavljanja djece na internetu.
20. S obzirom na to bi se obveze otkrivanja uvedene Prijedlogom primjenjivale samo na primatelje naloga za otkrivanje, bilo bi važno u tekstu predložene uredbe pojasniti da dobrovoljna upotreba tehnologija za otkrivanje materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece ostaje dopuštena samo u mjeri u kojoj je to dopušteno Direktivom o e-privatnosti i Općom uredbom o zaštiti podataka.

²⁹ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Tekst značajan za EGP) (SL L 119, 4.5.2016., str. 1.–88.).

³⁰ Presuda od 21. prosinca 2016., spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB i Watson*, t. 89.

To bi, na primjer, značilo da bi pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga bili spriječeni upotrebljavati takve tehnologije na dobrovoljnoj osnovi, osim ako bi to bilo dopušteno nacionalnim zakonima kojima se prenosi Direktive o e-privatnosti, u skladu s člankom 15. stavkom 1. Direktive o e-privatnosti i Poveljom.

21. Općenito, u predloženoj uredbi bilo bi korisno dodatno pojasniti status dobrovoljnog otkrivanja seksualnog zlostavljanja djece na internetu nakon datuma početka primjene predložene uredbe te prijelaz sa sustava dobrovoljnog otkrivanja utvrđenog u Privremenoj uredbi na obveze otkrivanja utvrđene u predloženoj uredbi. Na primjer, EDPB i EDPS preporučuju da se pojasni da se predloženom uredbom neće predvidjeti zakonita osnova za obradu osobnih podataka isključivo u svrhu dobrovoljnog otkrivanja seksualnog zlostavljanja djece na internetu.

4.2 [Zakonita osnova na temelju Opće uredbe o zaštiti podataka](#)

22. Prijedlogom se nastoji uspostaviti zakonita osnova, u smislu Opće uredbe o zaštiti podataka, za obradu osobnih podataka za potrebe otkrivanja materijala koji sadržava seksualno zlostavljanje djece i vrbovanja djece. U skladu s time, u obrazloženju se navodi sljedeće: „Kad je riječ o obveznim aktivnostima otkrivanja koje uključuju obradu osobnih podataka, Prijedlogom i osobito nalozima za otkrivanje izdanima na temelju njega uspostavlja se osnova za takvu obradu iz članka 6. stavka 1. točke (c) Opće uredbe o zaštiti podataka, kojom se predviđa obrada osobnih podataka nužna radi poštovanja pravnih obveza voditelja obrade na temelju prava Unije ili prava države članice.”³¹
23. EDPB i EDPS pozdravljaju odluku Komisije da ukloni pravnu nesigurnost u pogledu pravne osnove obrade osobnih podataka, koja je proizašla na temelju Privremene uredbe. EDPB i EDPS također se slažu sa zaključkom Komisije da su posljedice uvođenja mjera za otkrivanje previše dalekosežne i ozbiljne da bi se odluka o provedbi takvih mjera prepustila pružateljima usluga.³² EDPB i EDPS istodobno napominju da će svaka pravna osnova kojom se pružatelje usluga obvezuje na zadiranje u temeljna prava na zaštitu podataka i privatnosti biti valjana samo ako se njome poštuju uvjeti utvrđeni u članku 52. stavku 1. Povelje, kako je analizirano u sljedećim odjeljcima.

4.3 [Obveze procjene i ublažavanja rizika](#)

24. U skladu s poglavljem II., odjeljkom 1. Prijedloga, pružatelji usluga smještaja informacija na poslužitelju i pružatelji interpersonalnih komunikacijskih usluga dužni su za svaku uslugu koju pružaju utvrditi, analizirati i procijeniti rizik od upotrebe usluge u svrhu seksualnog zlostavljanja djece na internetu, a zatim pokušati umanjiti utvrđeni rizik primjenom „razumnih mjera za smanjenje rizika prilagođenih utvrđenom riziku”.
25. EDPB i EDPS napominju da bi pri provedbi procjene rizika pružatelj trebao posebno uzeti u obzir elemente navedene u članku 3. stavku 2. točkama od (a) do (e) Prijedloga, uključujući: zabrane i ograničenja utvrđena u uvjetima i odredbama pružatelja usluga; način na koji korisnici upotrebljavaju uslugu i utjecaj koji to ima na navedeni rizik; način na koji je pružatelj osmislio uslugu i upravlja njome, uključujući poslovni model, upravljanje te relevantne sustave i procese, i utjecaj koji to ima na navedeni rizik. Kad je riječ o riziku od mamljenja djece, potrebno je uzeti u obzir sljedeće predložene elemente: mjeru u kojoj uslugu upotrebljavaju ili je vjerojatno da će je upotrebljavati djeca; dobne skupine i rizik od mamljenja djece za te dobne skupine; dostupnost funkcionalnosti koje omogućuju korisnicima da traže druge korisnike, funkcionalnosti koje omogućuju korisnicima da izravno stupe u

³¹ Ibid., str. 4.

³² Usp. Prijedlog, COM(2022) 209 final, str. 14.

kontakt s drugim korisnicima, osobito putem privatnih komunikacija i funkcionalnosti koje korisnicima omogućuju razmjenu slika ili videozapisa s drugim korisnicima.

26. Iako EDPB i EDPS priznaju da se ti kriteriji čine relevantnima, EDPB i EDPS ipak su zabrinuti zbog toga što takvi kriteriji ostavljaju prilično širok prostor za tumačenje i slobodnu procjenu. Nekoliko kriterija opisano je izrazito općenitim pojmovima (npr. „način na koji korisnici upotrebljavaju uslugu i utjecaj koji to ima na navedeni rizik”) ili se odnose na osnovne funkcionalnosti koje su zajedničke mnogim internetskim uslugama (npr. „omogućuju korisnicima dijeljenje slika ili videozapisa s drugim korisnicima”). Kriteriji su kao takvi podložni subjektivnoj (a ne objektivnoj) procjeni.
27. EDPB i EDPS smatraju da isto vrijedi i za mjere za smanjenje rizika koje treba poduzeti u skladu s člankom 4. Prijedloga. Mjere kao što su prilagodba pružateljeva sustava za moderiranje sadržaja ili sustava za preporučivanje poduzimanjem odgovarajućih tehničkih i operativnih mjera te angažiranjem odgovarajućeg osoblja. Međutim, ako se primjenjuju u okviru složenog postupka procjene rizika i u kombinaciji s apstraktnim i nejasnim pojmovima kako bi se opisala prihvatljiva količina rizika (npr. „znatna mjera”), ti kriteriji ne ispunjavaju kriterije pravne sigurnosti i predvidljivosti koji su potrebni za opravdanje zadiranja u povjerljivost komunikacija između pojedinaca, što predstavlja jasno zadiranje u temeljna prava na privatnost i slobodu izražavanja.
28. Iako pružatelji usluga nisu ovlašteni zadirati u povjerljivost komunikacija u okviru svojih strategija procjene i smanjenja rizika prije primanja naloga za otkrivanje, postoji izravna veza između obveza procjene i smanjenja rizika te obveza otkrivanja koje iz toga proizlaze. Na temelju članka 7. stavka 4. Prijedloga izdavanje naloga za otkrivanje ovisi o postojanju dokaza o znatnom riziku da bi se relevantna usluga mogla upotrebljavati u svrhu seksualnog zlostavljanja djece na internetu. Prije izdavanja naloga za otkrivanje potrebno je slijediti složen postupak koji uključuje pružatelje usluga, koordinacijsko tijelo i pravosudno ili drugo neovisno upravno tijelo odgovorno za izdavanje naloga. Prvo, pružatelji usluga moraju procijeniti rizik od upotrebe svojih usluga u svrhe seksualnog zlostavljanja djeteta na internetu (članak 3. Prijedloga) i ocijeniti moguće mjere smanjenja rizika (članak 4. Prijedloga) kako bi se taj rizik smanjio. Rezultate tog postupka zatim treba dostaviti nadležnom koordinacijskom tijelu (članak 5. Prijedloga). Ako procjena rizika pokaže da i dalje postoji znatan rizik unatoč nastojanjima da ga se ublaži, koordinacijsko tijelo mora saslušati mišljenje pružatelja usluga o nacrtu zahtjeva za izdavanje naloga za otkrivanje i mora pružatelju usluga dati mogućnost da iznese primjedbe. Nadalje, pružatelj je dužan predstaviti plan provedbe, uključujući mišljenje nadležnog tijela za zaštitu podataka u slučaju otkrivanja mamljenja. Ako koordinacijsko tijelo nastavi s predmetom, traži se izdavanje naloga za otkrivanje koji na kraju izdaje sud ili drugo neovisno upravno tijelo. Stoga su početna procjena rizika i mjere odabrane za utvrđivanje rizika odlučujuća osnova za procjenu potrebe izdavanja naloga za otkrivanje koju provode koordinacijsko tijelo i nadležno pravosudno ili upravno tijelo.
29. EDPB i EDPS svjesni su složenih koraka koji vode do izdavanja naloga za otkrivanje, a koji uključuju početnu procjenu rizika koju provodi pružatelj usluga i prijedlog pružatelja usluga o mjerama za smanjenje rizika, kao i daljnju interakciju pružatelja usluga s nadležnim koordinacijskim tijelom. EDPB i EDPS smatraju da postoji znatna mogućnost da pružatelj usluga utječe na ishod postupka. U tom pogledu EDPB i EDPS napominju da se u uvodnoj izjavi 17. Prijedloga propisuje da bi pružatelji usluga trebali moći, kao dio izvješćivanja o rizicima, navesti „svoju želju i spremnost” da im se izda nalog za otkrivanje. Stoga se ne može pretpostaviti da će svaki pružatelj usluga nastojati izbjeći izdavanje naloga za otkrivanje kako bi se zadržala povjerljivost komunikacija njegovih korisnika primjenom najučinkovitijih, ali i najmanje nametljivih mjera smanjenja rizika, osobito kad takve mjere smanjenja rizika zadiru u slobodu poduzetništva pružatelja usluga u skladu s člankom 16. Povelje.

30. EDPS i EDPB žele naglasiti da postupovne zaštitne mjere ne mogu nikada u potpunosti zamijeniti materijalne zaštitne mjere. Stoga bi prethodno opisani složeni postupak koji vodi do mogućeg izdavanja naloga za otkrivanje trebao biti popraćen jasnim materijalnim obvezama. EDPB i EDPS smatraju da Prijedlog nije dovoljno jasan u pogledu nekoliko ključnih elemenata (npr. pojmovi „znatan rizik“, „znatna mjera“ itd.), koji se ne mogu ispraviti postojanjem višeslojnih postupovnih zaštitnih mjera. Navedeno je još važnije s obzirom na činjenicu da subjekti zaduženi za primjenu tih zaštitnih mjera (npr. pružatelji usluga, pravosudna tijela itd.) imaju širok prostor za slobodnu procjenu načina na koji postići ravnotežu između prava o kojima je riječ u svakom pojedinačnom slučaju. S obzirom na opsežna zadiranja u temeljna prava koja bi proizašla iz donošenja Prijedloga, zakonodavac bi trebao osigurati da se Prijedlogom pruži veća jasnoća o tome kada i gdje su takva zadiranja dopuštena. Iako priznaju da zakonodavne mjere ne mogu biti previše preskriptivne i mora se ostaviti određena fleksibilnost u njihovoj praktičnoj primjeni, EDPB i EDPS smatraju da je Prijedlogu ostavljeno previše prostora za moguću zlouporabu zbog nepostojanja jasnih materijalnih normi.
31. S obzirom na mogući znatan učinak na vrlo velik broj ispitanika (tj. potencijalno sve korisnike interpersonalnih komunikacijskih usluga), EDPB i EDPS ističu potrebu za visokom razinom sigurnosti, jasnoće i predvidljivosti zakonodavstva kako bi se osigurala istinska učinkovitost predloženih mjera u postizanju cilja koji se nastoji postići te njihov najmanji negativni učinak na predmetna temeljna prava.

4.4 Uvjeti za izdavanje naloga za otkrivanje

32. Člankom 7. Prijedloga predviđa se da će koordinacijsko tijelo u državi poslovnog nastana imati ovlast od nadležnog pravosudnog tijela ili drugog neovisnog upravnog tijela te države članice zatražiti izdavanje naloga za otkrivanje kojim se od pružatelja usluga smještaja informacija na internetu ili pružatelja interpersonalnih komunikacijskih usluga zahtijeva da na određenoj usluzi poduzme mjere za otkrivanje seksualnog zlostavljanje djece na internetu, koje su utvrđene u članku 10.
33. EDPB i EDPS uzimaju u obzir sljedeće elemente koje treba ispuniti prije izdavanja naloga za otkrivanje:
- postoje dokazi o znatnom riziku od upotrebe usluge u svrhu seksualnog zlostavljanja djece na internetu u smislu članka 7. stavaka 5., 6. i 7., ovisno o slučaju;
 - razlozi za izdavanje naloga za otkrivanje nadilaze negativne posljedice za prava i legitimne interese svih osoba na koje se taj nalog odnosi, posebno uzimajući u obzir potrebu da se osigura pravedna ravnoteža između temeljnih prava tih osoba.
34. Značenje znatnog rizika određeno je stavkom 5. i člankom 7., ovisno o vrsti nalog za otkrivanje koji se razmatra. U slučaju naloga za otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece, pretpostavlja se da postoji znatan rizik ako su ispunjeni sljedeći uvjeti:
- vjerojatno je, unatoč svim mjerama za smanjenje rizika koje je pružatelj eventualno poduzeo ili će poduzeti, da se usluga u znatnoj mjeri upotrebljava za širenje poznatog materijala koji sadržava seksualno zlostavljanje djece i
 - postoje dokazi da se usluga ili usporediva usluga, ako se ta usluga još ne nudi u Uniji na datum kad je zatraženo izdavanje naloga za otkrivanje, u posljednjih 12 mjeseci i u znatnoj mjeri upotrebljava za širenje poznatog materijala koji sadržava seksualno zlostavljanje djece.
35. Kako bi se izdao nalog za otkrivanje nepoznatog materijala koji sadržava seksualno zlostavljanje djece, vjerojatnost i činjenični dokazi moraju upućivati na nepoznati materijal koji sadržava seksualno zlostavljanje djece, prethodno je izdan nalog za otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece, a pružatelj usluga na temelju njega dostavio je veliki broj prijava materijala koji

sadržava seksualno zlostavljanje djece (članak 7. stavak 6. Prijedloga). Kad je riječ o nalogu za otkrivanje vrbovanja, smatrat će se da postoji znatan rizik ako se pružatelj usluga smatra pružateljem interpersonalnih komunikacijskih usluga, ako je vjerojatno da se usluga u znatnoj mjeri upotrebljava za mamljenje djece i ako postoje dokazi da se usluga u znatnoj mjeri upotrebljava za mamljenje djece (članak 7. stavak 7. Prijedloga).

36. EDPB i EDPS primjećuju da čak i uz specifikacije iz članka 5. stavaka od 5. do 7. Prijedloga uvjetima za izdavanje naloga za otkrivanje prevladavaju nejasni pravni pojmovi, kao što su „znatna mjera”, „veliki broj”, i djelomično se ponavljaju jer će dokazi o prethodnoj zlouporabi često pridonijeti utvrđivanju vjerojatnosti buduće zlouporabe.
37. Prijedlogom se predviđa sustav u okviru kojeg je pri odlučivanju o potrebi naloga za otkrivanje potrebno donijeti odluku o predviđanju buduće upotrebe usluge u svrhu seksualnog zlostavljanje djece na internetu. Stoga je razumljivo da su elementi utvrđeni u članku 7. po prirodi prognostičke prirode. Međutim, primjena nejasnih pojmova u Prijedlogu pružateljima usluga, kao i nadležnom pravosudnom ili drugom ovlaštenom neovisnom upravnom tijelu, otežava primjenu pravnih zahtjeva uvedenih Prijedlogom na predvidljiv i neproizvoljan način. EDPB i EDPS zabrinuti su da će ti općeniti i nejasni pojmovi dovesti do nedostatka pravne sigurnosti i do znatnih razlika u konkretnoj provedbi Prijedloga u Uniji, ovisno o tumačenju pojmova kao što su „vjerojatnost” i „znatna mjera” u pravosudnim ili drugim neovisnim upravnim tijelima država članica. Takav ishod ne bi bio prihvatljiv s obzirom na činjenicu da će odredbe o nalogima za otkrivanje za pružatelje interpersonalnih komunikacijskih usluga predstavljati „ograničenja” načela povjerljivosti komunikacija utvrđenog u članku 5. Direktive o e-privatnosti te su stoga njihova jasnoća i predvidljivost od iznimne važnosti kako bi se osigurala ujednačena primjena tih ograničenja u Uniji.

4.5 Analiza nužnosti i proporcionalnosti predviđenih mjera³³

38. Kako je prethodno naznačeno, postoje tri vrste naloga za otkrivanje koji se mogu izdati: nalozi za otkrivanje koji se odnose na širenje poznatog materijala koji sadržava seksualno zlostavljanje djece (članak 7. stavak 5. Prijedloga), nalozi za otkrivanje koji se odnose na širenje novog materijala koji sadržava seksualno zlostavljanje djece (članak 7. stavak 6. Prijedloga) i nalozi za otkrivanje koji se odnose na mamljenje djece (članak 7. stavak 7. Prijedloga). Za svaki nalog za otkrivanje obično bi bila potrebna drukčija tehnologija za njegovu praktičnu primjenu. Stoga imaju različitu razinu narušavanja privatnosti, a time i različit učinak na prava na privatnost i zaštitu osobnih podataka.
39. Tehnologije za otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece najčešće su tehnologije koje se podudaraju u smislu da se oslanjaju na postojeću bazu podataka poznatog materijala koji sadržava seksualno zlostavljanje djece na temelju koje mogu usporediti slike (uključujući fotografije iz videozapisa). Kako bi se omogućilo uspoređivanje, slike koje pružatelj usluga obrađuje i slike u bazi podataka moraju biti digitalne, najčešće dobivene pretvaranjem u vrijednosti raspršivanja („hash”). Ta vrsta tehnologija raspršivanja ima procijenjenu stopu lažno pozitivnih rezultata od najviše 1 na 50 milijardi (tj. 0,000000002 % lažno pozitivnih rezultata).³⁴

³³ Vidjeti i „Brzi vodič EDPS-a o nužnosti i proporcionalnosti”, dostupan na: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

³⁴ Vidjeti Radni dokument službi Komisije, Izvješće o procjeni učinka priloženo Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece, SWD(2022) 209 final (dalje u tekstu: „Izvješće o procjeni učinka” ili „SWD(2022) 209 final”), str. 281., fn. 511.

40. Za otkrivanje novog materijala koji sadržava seksualno zlostavljanje djece obično se upotrebljava različita vrsta tehnologije, uključujući klasifikatore i umjetnu inteligenciju (UI).³⁵ Međutim, njihove su stope pogreške općenito znatno više. Na primjer, u Izvješću o procjeni učinka navodi se da postoje tehnologije za otkrivanje novog materijala koji sadržava seksualno zlostavljanje djece čija se stopa preciznosti može odrediti na 99,9 % (tj. 0,1 % lažno pozitivnih rezultata), ali s tom preciznošću mogu utvrditi samo 80 % ukupnog materijala koji sadržava seksualno zlostavljanje djece u relevantnom skupu podataka.³⁶
41. Kad je riječ o otkrivanju mamljenja djece u tekstualnim komunikacijama, u Izvješću o procjeni učinka objašnjava se da se to obično temelji na otkrivanju uzoraka. U izvješću o procjeni učinka navodi se da neke od postojećih tehnologija za otkrivanje vrbovanja imaju „stopu preciznosti” od 88 %³⁷. Prema mišljenju Komisije, to znači da „od 100 razgovora označenih kao moguće kazneno djelo mamljenja djece njih 12 [EU-ov centar] može isključiti nakon pregleda [u skladu s Prijedlogom] i neće se prijaviti tijelima za izvršavanje zakonodavstva”.³⁸ Međutim, iako bi se Prijedlog, za razliku od Privremene uredbe, primjenjivao i na audiokomunikacije, u Izvješću o procjeni učinka nisu razrađena tehnološka rješenja koja bi se mogla upotrijebiti za otkrivanje vrbovanja u takvom okruženju.

4.5.1 Djelotvornost otkrivanja

42. Nužnost podrazumijeva potrebu za činjenično utemeljenom procjenom djelotvornosti predviđenih mjera za postizanje željenog cilja i toga narušava li se njome privatnost u manjoj mjeri nego drugim mogućnostima za postizanje istog cilja.³⁹ Drugi čimbenik koji treba uzeti u obzir pri procjeni proporcionalnosti predložene mjere jest djelotvornost postojećih mjera u odnosu na one predložene.⁴⁰ Ako već postoje mjere u istu ili sličnu svrhu, njihovu djelotvornost treba procijeniti kao dio procjene proporcionalnosti. Bez takve procjene djelotvornosti postojećih mjera koje imaju istu ili sličnu svrhu ne može se smatrati da je test proporcionalnosti za novu mjeru propisno proveden.
43. Otkrivanjem materijala koji sadržava seksualno zlostavljanje djece ili vrbovanje koje provode pružatelji usluga smještaja informacija na poslužitelju i pružatelji interpersonalnih komunikacijskih usluga može se pridonijeti općem cilju sprečavanja i suzbijanja seksualnog zlostavljanja djece i širenja materijala koji sadržava seksualno zlostavljanje djece na internetu. Istodobno, potreba za procjenom djelotvornosti mjera predviđenih Prijedlogom nameće tri ključna pitanja:
- Mogu li se mjere za otkrivanje seksualnog zlostavljanja djece na internetu jednostavno izbjeći?
 - Kakav će učinak aktivnosti otkrivanja imati na mjere koje poduzimaju tijela za izvršavanje zakonodavstva?⁴¹

³⁵ Izvješće o procjeni učinka, str. 281.

³⁶ Ibid., str. 282.

³⁷ Ibid., str. 283.

³⁸ Prijedlog, COM(2022) 209 final, str. 14., fn. 32.

³⁹ EDPS, Procjena nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka: skup alata, 11. travnja 2017., str. 5.; EDPS, Smjernice Europskog nadzornika za zaštitu podataka o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka (19. prosinca 2019.), str. 8.

⁴⁰ EDPS, Smjernice Europskog nadzornika za zaštitu podataka o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka (19. prosinca 2019.), str. 11.

⁴¹ Prema Prilogu II. Izvješću o procjeni učinka, str. 132., 85,71 % ispitanika u istraživanju o kaznenom progonu izrazilo je zabrinutosti zbog povećanog broja materijala koji sadržava seksualno zlostavljanje djece u posljednjem desetljeću i nedostatka resursa (tj. ljudskih i tehničkih).

- Kako bi se Prijedlogom smanjila pravna nesigurnost?

44. Nije na EDPB-u i EDPS-u da detaljno odgovore na ta pitanja. Međutim, EDPB i EDPS napominju da se ni u Izvješću o procjeni učinka ni u Prijedlogu na ta pitanja ne odgovora u potpunosti.
45. Kad je riječ o mogućnosti izbjegavanja otkrivanja materijala koji sadržava seksualno zlostavljanje djece, treba napomenuti da se čini da trenutačno ne postoji tehnološko rješenje za otkrivanje materijala koji sadržava seksualno zlostavljanje djece koji se dijeli u šifriranom obliku. Stoga se svaka aktivnost otkrivanja, čak i pregled na strani klijenta čija je namjena izbjeći šifriranje s kraja na kraj koje nudi pružatelj usluga⁴², može jednostavno izbjeći šifriranjem sadržaja s pomoću zasebne aplikacije prije njegova slanja ili učitavanja. Stoga bi mjere za otkrivanje predviđene Prijedlogom mogle imati manji učinak na širenje materijala koji sadržava seksualno zlostavljanje djece na internetu nego što bi se moglo očekivati.
46. Nadalje, uvođenjem obveza otkrivanja predviđenih Prijedlogom Komisija očekuje povećanje broja prijava seksualnog zlostavljanja djece tijelima za izvršavanje zakonodavstva.⁴³ Međutim, ni u Prijedlogu ni u Izvješću o procjeni učinka ne objašnjava se kako će se time otkloniti nedostaci trenutačnog stanja. S obzirom na ograničene resurse u tijelima za izvršavanje zakonodavstva, čini se potrebnim bolje razumjeti bi li povećanje broja prijava imalo značajan učinak na aktivnosti kaznenog progona protiv seksualnog zlostavljanja djece. U svakom slučaju, EDPB i EDPS žele naglasiti da bi se takve prijave trebale pravodobno ocijeniti kako bi se osiguralo da se odluka o kaznenoj relevantnosti prijavljenog materijala donese što prije i kako bi se što je više moguće ograničilo zadržavanje nevažnih podataka.

4.5.2 Ne postoji mjera koja manje narušava privatnost

47. Pod pretpostavkom da je moguće ostvariti pozitivne učinke otkrivanja materijala koji sadržava seksualno zlostavljanje djece i vrbovanja koje je predvidjela Komisija, otkrivanje mora biti mjera koja najmanje narušava privatnost među jednako učinkovitim mjerama. Člankom 4. Prijedloga predviđa se da bi, kao prvi korak, pružatelji usluga trebali razmotriti donošenje mjera za smanjenje rizika kako bi se rizik od upotrebe njihovih usluga u svrhu seksualnog zlostavljanja djece na internetu smanjio ispod praga kojim se opravdava izdavanje naloga za otkrivanje. Ako postoje mjere za smanjenje rizika koje bi mogle dovesti do znatnog smanjenja vrbovanja ili količine materijala koji sadržava seksualno zlostavljanje djece koji se razmjenjuje unutar relevantne usluge, te bi mjere često predstavljale mjere koje manje narušavaju privatnost u usporedbi s nalogom za otkrivanje⁴⁴. Stoga, ako relevantni pružatelj usluga ne donese takve mjere na dobrovoljnoj osnovi, nadležno neovisno upravno tijelo ili pravosudno tijelo trebalo bi moći provedbu mjera za smanjenje rizika učiniti obveznom i izvršivom umjesto izdavanja naloga za otkrivanje. EDPB i EDPS smatraju da činjenica da se člankom 5. stavkom 4. Prijedloga koordinacijskom tijelu omogućuje da od pružatelja usluga „zahtijeva” uvođenje, preispitivanje, ukidanje ili proširenje mjera za smanjenje rizika nije dovoljna jer takav zahtjev ne bi bio neovisno provediv; nepridržavanje bi se „sankcioniralo” samo izdavanjem naloga za otkrivanje.

⁴² Vidjeti i odjeljak 4.10. u nastavku.

⁴³ Vidjeti, među ostalim, Izvješće o procjeni učinka, Prilog 3., SWD(2022) 209 final, str. 176.

⁴⁴ Na primjer, trebalo bi razmotriti mjere poput onemogućivanja prijenosa materijala koji sadržava seksualno zlostavljanje djece na strani klijenta sprečavanjem učitavanja i slanja sadržaja elektroničkih komunikacija jer bi one u određenim kontekstima mogle pomoći spriječiti optjecaj poznatog materijala koji sadržava seksualno zlostavljanje djece.

48. Stoga EDPB i EDPS smatraju da bi koordinacijsko tijelo ili nadležno neovisno upravno ili pravosudno tijelo trebalo izričito ovlastiti za izricanje mjera za smanjenje rizika koje manje narušavaju privatnost prije ili umjesto izdavanja naloga za otkrivanje.

4.5.3 Proporcionalnost u užem smislu

49. Kako bi mjera bila u skladu s načelom proporcionalnosti iz članka 52. stavka 1. Povelje, prednosti koje proizlaze iz mjere ne bi smjele biti manje od nedostataka koje mjere uzrokuju u pogledu ostvarivanja temeljnih prava. Stoga, načelo proporcionalnosti „ograničuje tijela u izvršavanju njihovih ovlasti zahtijevajući da se uspostavi ravnoteža između upotrijebljenih sredstava i željenog cilja (ili postignutog rezultata)”.⁴⁵
50. Kako bi se mogao procijeniti učinak mjere na temeljna prava na privatnost i zaštitu osobnih podataka, posebno je važno precizno utvrditi sljedeće: ⁴⁶
- **područje primjene mjere**, uključujući broj osoba na koje se mjera odnosi i izaziva li ona „kolateralna zadiranja” (tj. zadiranje u privatnost osoba koje nisu subjekti mjere);
 - **opseg mjere**, uključujući količinu prikupljenih informacija; trajanje; zahtijeva li mjera koja se ispituje prikupljanje i obradu posebnih kategorija podataka;
 - **razinu narušavanja privatnosti**, uzimajući u obzir prirodu aktivnosti koja podliježe mjeri (odnosi li se na aktivnosti obuhvaćene obvezom povjerljivosti, odnos između odvjetnika i klijenta; medicinsku djelatnost); kontekst; je li riječ o izradi profila pojedinaca; podrazumijeva li obrada (djelomičnu ili potpunu) upotrebu sustava automatiziranog donošenja odluka s „dopuštenim odstupanjem”;
 - odnosi li se na **ranjive osobe**;
 - utječe li i na **druga temeljna prava** (na primjer pravo na slobodu izražavanja, kao u predmetima *Digital Rights Ireland* i *Seitlinger i dr. te Tele2 Sverige i Watson*).⁴⁷
51. U tom je kontekstu također važno napomenuti da učinak može biti neznatan za dotičnog pojedinca, ali ipak značajan ili vrlo značajan kolektivno/za društvo u cjelini.⁴⁸
52. U svim trima vrstama naloga za otkrivanje (otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece, novog materijala koji sadržava seksualno zlostavljanje djece i vrbovanja), trenutno dostupne tehnologije oslanjaju se na automatiziranu obradu podataka o sadržaju svih korisnika na koje se to odnosi. Tehnologije koje se upotrebljavaju za analizu sadržaja često su složene

⁴⁵ Vidjeti predmet C-343/09, *Afton Chemical*, t. 45.; spojene predmete C-92/09 i C-93/09, *Volker und Markus Schecke i Hartmut Eifert*, t. 74.; predmete C-581/10 i C-629/10, *Nelson i dr.*, t. 71.; predmet C-283/11, *Sky Österreich*, t. 50.; i predmet C-101/12, *Schaible*, t. 29. Vidjeti i EDPS, Procjena nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka: skup alata (11. travnja 2017.).

⁴⁶ EDPS, Smjernice o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka (19. prosinca 2019.), str. 23.

⁴⁷ Vidjeti i Mišljenje 7/20202 Europskog nadzornika za zaštitu podataka o Prijedlogu privremenih odstupanja od Direktive 2022/58/EZ u svrhu protiv seksualnog zlostavljanje djece na internetu (10. studenoga 2020.), t. 9. i dalje.

⁴⁸ EDPS, Smjernice o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka (19. prosinca 2019.), str. 20.

i obično uključuju upotrebu umjetne inteligencije. Kao posljedica navedenog, ponašanje te tehnologije možda neće biti u potpunosti razumljivo korisniku usluge. Nadalje, poznato je da trenutačno dostupne tehnologije, osobito one za otkrivanje novog materijala koji sadržava seksualno zlostavljanje djece ili vrbovanja, imaju relativno visoke stope pogreške.⁴⁹ Osim toga, postoji rizik da se o tome izvjesti EU-ov centar u skladu s člankom 12. stavkom 1. i člankom 48. stavkom 1. Prijedloga, na temelju otkrivanja „potencijalnog” materijala koji sadržava seksualno zlostavljanje djece.

53. Nadalje, opći uvjeti za izdavanje naloga za otkrivanje na temelju Prijedloga, tj. oni koji se primjenjuju na cijelu uslugu, a ne samo na odabrane komunikacije⁵⁰, trajanje do 24 mjeseci za poznati ili novi materijal koji sadržava seksualno zlostavljanje djece i do 12 mjeseci za vrbovanje⁵¹ itd., mogu u praksi dovesti do vrlo širokog opsega naloga. Stoga bi praćenje zapravo bilo opće i neselektivno, a u praksi ne bi bilo ciljano.
54. S obzirom na navedeno, EDPB i EDPS zabrinuti su i zbog mogućih odvrćajućih učinaka na ostvarivanje slobode izražavanja. EDPB i EDPS podsjećaju da se takav odvrćajućii učinak smatra vjerojatnijim što je zakon manje jasan.
55. U nedostatku specifičnosti, preciznosti i jasnoće koje su potrebne kako bi se ispunio zahtjev pravne sigurnosti⁵², i s obzirom na široko područje primjene, tj. sve pružatelje relevantnih usluga informacijskog društva koji pružaju takve usluge u Uniji⁵³, Prijedlogom se ne osigurava učinkovita provedba isključivo ciljanog pristupa otkrivanju materijala koji sadržava seksualno zlostavljanje djece i vrbovanja. Stoga EDPB i EDPS smatraju da bi u praksi Prijedlog mogao postati temelj za *de facto* opće i neselektivno pregledavanje sadržaja gotovo svih vrsta elektroničkih komunikacija svih korisnika u EU-u/EGP-u. Kao rezultat navedenog, zakonodavstvo može dovesti do toga da se ljudi suzdržavaju od dijeljenja zakonitog sadržaja zbog straha da će biti na udaru zbog svoje aktivnosti.
56. Međutim, EDPB i EDPS svjesni su da različite mjere za suzbijanje seksualnog zlostavljanje djece na internetu mogu uključivati različite razine narušavanja privatnosti. Kao prvo, EDPB i EDPS primjećuju da će automatizirana analiza govora ili teksta u cilju utvrđivanja mogućih slučajeva mamljenja djece vjerojatno predstavljati značajnije zadiranje od povezivanja slika ili videozapisa na temelju prethodno potvrđenih slučajeva materijala koji sadržava seksualno zlostavljanje djece u cilju otkrivanja širenja materijala koji sadržava seksualno zlostavljanje djece. Nadalje, potrebno je razlikovati otkrivanje „poznatog materijala koji sadržava seksualno zlostavljanje djece” i „novog materijala koji sadržava seksualno zlostavljanje djece”. Osim toga, učinak bi trebalo dodatno razlikovati u pogledu mjera protiv pružatelja usluga smještaja informacija na poslužitelju i mjera nametnutih pružateljima interpersonalnih komunikacijskih usluga.

4.5.4 Otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece

57. Iako bi u skladu s uvodnom izjavom 4. Prijedlog bio „tehnološki neutralan”, djelotvornost predloženih mjera za otkrivanje i njihov učinak na pojedince uvelike će ovisiti o odabiru primijenjene tehnologije i o odabranim pokazateljima. Komisija je tu činjenicu potvrdila u Prilogu 8. izvješću o procjeni učinka⁵⁴,

⁴⁹ Vidjeti prethodno navedene pojedinosti, odjeljak 4.5., i pododjeljak 4.8.2 u nastavku.

⁵⁰ Vidjeti članak 7. stavak 1. Prijedloga.

⁵¹ Vidjeti članak 7. stavak 9. treći podstavak Prijedloga.

⁵² Us p. Sud EU-a, predmet C-197/96, *Komisija Europskih zajednica protiv Francuske Republike*, t. 15.

⁵³ Vidjeti članak 1. stavak 2. Prijedloga.

⁵⁴ Us p. i informacije o stopama lažno pozitivnih rezultata u Izvješću o procjeni učinka, Prilog 8., str. 279. i dalje.

a potvrdile su je i druge studije, kao što je procjena ciljanog učinka zamjenske mjere koju je provela Služba Europskog parlamenta za istraživanja o prijedlogu Komisije o privremenom odstupanju od Direktive o e-privatnosti u svrhu suzbijanja zlostavljanja djece na internetu od veljače 2021.⁵⁵

58. U članku 10 Prijedloga utvrđuje se broj zahtjeva za tehnologije koje se će upotrebljavati u svrhu otkrivanja, osobito u pogledu njihove djelotvornosti, pouzdanosti i prirode koja najmanje narušava privatnost u smislu učinka na prava korisnika na privatni i obiteljski život, uključujući povjerljivost komunikacija, te na zaštitu osobnih podataka.
59. U tom kontekstu EDPB i EDPS napominju da su trenutačno jedine tehnologije za koje se čini da mogu općenito ispuniti te standarde one koje se upotrebljavaju za otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece, tj. tehnologije prepoznavanja koje se oslanjaju na bazu podataka raspršivanja kao referentnu vrijednost.

4.5.5 Otkrivanje prethodno nepoznatog materijala koji sadržava seksualno zlostavljanje djece

60. Procjena mjera usmjerenih na otkrivanje prethodno nepoznatog (novog) materijala koji sadržava seksualno zlostavljanje djece dovodi do različitih zaključaka o njihovoj djelotvornosti, pouzdanosti i ograničenju učinka na temeljna prava na privatnost i zaštitu podataka.
61. Prvo, kako je objašnjeno u Izvješću o procjeni učinka priloženom Prijedlogu, tehnologije koje se trenutačno upotrebljavaju za otkrivanje prethodno nepoznatog materijala koji sadržava seksualno zlostavljanje djece uključuju klasifikatore i umjetnu inteligenciju. Klasifikator je algoritam kojim se podatci razvrstavaju u označene razrede ili kategorije informacija prepoznavanjem uzoraka.⁵⁶ Stoga te tehnologije imaju različite rezultate i učinak u smislu točnosti, djelotvornosti i razine narušavanja privatnosti. Istodobno su i podložnije pogreškama.
62. Tehnike koje se upotrebljavaju za otkrivanje prethodno nepoznatog materijala koji sadržava seksualno zlostavljanje djece slične su onima koje se upotrebljavaju za otkrivanje mamljenja djece jer se nijedna ne temelji na jednostavnim tehnologijama prepoznavanja, nego na prediktivnim modelima u kojima se upotrebljavaju tehnologije umjetne inteligencije. EDPB i EDPS smatraju da je pri otkrivanju prethodno nepoznatog materijala koji sadržava seksualno zlostavljanje djece potreban izrazit oprez jer bi pogreška sustava imala ozbiljne posljedice za ispitanike, koji bi automatski bili označeni da su možda počinili vrlo teško kazneno djelo te bi došlo do prijave njihovih osobnih podataka i pojedinosti njihove komunikacije.
63. Drugo, pokazatelji uspješnosti utvrđeni u literaturi, od kojih su neki istaknuti u Izvješću o procjeni učinka priloženom Prijedlogu⁵⁷, pružaju vrlo malo informacija o uvjetima koji su upotrijebljeni za njihov izračun i njihovoj primjerenosti stvarnim uvjetima, što znači da bi njihova stvarna uspješnost mogla biti znatno niža od očekivane, što bi dovelo do manje točnosti i većeg postotka „lažnih pozitivnih rezultata”.
64. Treće, pokazatelje uspješnosti trebalo bi razmotriti u specifičnom kontekstu upotrebe relevantnih alata za otkrivanje i oni bi trebali pružiti iscrpan uvid u ponašanje alata za otkrivanje. Kada se na slike

⁵⁵ Usp. Prijedlog Komisije o privremenom odstupanju od Direktive o e-privatnosti u svrhu suzbijanja seksualnog zlostavljanja djece na internetu: procjena ciljanog učinka zamjenske mjere (Služba Europskog parlamenta za istraživanje, veljača 2021.), str. 14. i dalje.

⁵⁶ Izvješće o procjeni učinka, Prilog 8., str. 281.

⁵⁷ Izvješće o procjeni učinka, Prilog 8., str. 281.–283.

ili tekst primjenjuju algoritmi umjetne inteligencije, postoje brojni dokazi da, zbog nedostatka zastupljenosti određenih skupina stanovništva u podacima koji se upotrebljavaju za učenje algoritma, može doći do predrasuda i diskriminacije. Te bi pristranosti trebalo utvrditi, izmjeriti i smanjiti na prihvatljivu razinu kako bi sustavi za otkrivanje bili istinski korisni za društvo u cjelini.

65. Iako je provedena studija o tehnologijama koje se upotrebljavaju za otkrivanje⁵⁸, EDPB i EDPS smatraju da je potrebna daljnja analiza kako bi se procijenila pouzdanost postojećih alata. Ta bi se analiza trebala temeljiti na iscrpnim pokazateljima uspješnosti i procijeniti učinak mogućih pogrešaka u uvjetima stvarnog života na sve ispitanike obuhvaćene Prijedlogom.
66. Kako je prethodno navedeno, EDPB i EDPS ozbiljno sumnjaju u dostatnost postupovnih zaštitnih mjera iz članka 7. stavka 6. Prijedloga u smislu neutraliziranja tih rizika. Nadalje, kako je prethodno navedeno, napominju da se u Prijedlogu upotrebljavaju prilično apstraktni i nejasni pojmovi kako bi se opisala prihvatljiva količina rizika (npr. „znatna mjera”).
67. EDPB i EDPS zabrinuti su da će ti općeniti i nejasni pojmovi dovesti do nedostatka pravne sigurnosti i do znatnih razlika u konkretnoj provedbi Prijedloga u Uniji, ovisno o tome na koji će način pravosudna ili druga neovisna upravna tijela u državama članicama tumačiti pojmove kao što su „vjerojatnost” i „znatna mjera”. To je zabrinjavajuće i zbog činjenice da će odredbe o nalogima za otkrivanje predstavljati „ograničenja” načela povjerljivosti utvrđenog u članku 5. Direktive o e-privatnosti. Stoga je njihovu jasnoću i predvidljivost potrebno poboljšati u predloženoj uredbi.

4.5.6 Otkrivanje mamljenja („vrbovanja”) djece

68. EDPB i EDPS primjećuju da će predložene mjere koje se odnose na otkrivanje mamljenja djece („vrbovanje”), koje uključuju automatiziranu analizu govora ili teksta, vjerojatno predstavljati najveće zadiranje u prava korisnika na privatan i obiteljski život, uključujući povjerljivost komunikacija, i na zaštitu osobnih podataka.
69. Iako se otkrivanje poznatog, pa čak i novog materijala koji sadržava seksualno zlostavljanje djece može ograničiti na analizu slika i videozapisa, otkrivanje vrbovanja bi se po definiciji proširilo na sve tekstualne (a možda i audio) komunikacije koje su obuhvaćene područjem primjene naloga za otkrivanje. Zbog toga je intenzitet zadiranja u povjerljivost predmetnih komunikacija mnogo veći.
70. EDPB i EDPS smatraju da *de facto* opća i neselektivna automatizirana analiza tekstualne komunikacije koja se prenosi interpersonalnim komunikacijskim uslugama u cilju utvrđivanja mogućeg mamljenja djece ne poštuje zahtjeve nužnosti i proporcionalnosti. Čak i ako je tehnologija koja se upotrebljava ograničena na upotrebu pokazatelja, EDPB i EDPS smatraju da je primjena takve opće i neselektivne analize pretjerana i može utjecati na samu bit temeljnog prava na privatnost iz članka 7 Povelje.
71. Kao što je već navedeno, nedostatak postupovnih zaštitnih mjera u kontekstu mjera za otkrivanje mamljenja djece ne može se u potpunosti nadoknaditi samo postupovnim zaštitnim mjerama. Nadalje, problem nedostatka dostatne pravne jasnoće i sigurnosti (npr. upotreba nejasnog pravnog jezika poput „znatna mjera”) još je ozbiljniji u slučaju automatizirane analize tekstualne osobne komunikacije, u odnosu na usporedbu fotografija koja se temelji na tehnologiji raspršivanja.

⁵⁸ Izvješće o procjeni učinka, str. 279. i dalje.

72. Nadalje, EDPB i EDPS smatraju da je „učinak odvrtaćanja” na slobodu izražavanja posebno značajan kada se tekstualne (ili audio) komunikacije pojedinaca pregledavaju i analiziraju u velikim razmjerima. EDPB i EDPS podsjećaju da je takav odvrtaćajući učinak ozbiljniji što je zakon manje jasan.
73. Osim toga, kako je navedeno u Izvješću o procjeni učinka⁵⁹ i u studiji Službe Europskog parlamenta za istraživanja⁶⁰, stopa točnosti tehnologija za otkrivanje tekstualnog vrbovanja znatno je niža od stope točnosti tehnologija za otkrivanje poznatog materijala koji sadržava seksualno zlostavljanje djece⁶¹. Tehnike za otkrivanje vrbovanja djece osmišljene su za analizu i dodjelu ocjena vjerojatnosti svakom aspektu razgovora, stoga EDPB i EDPS također smatraju da su podložni pogreškama i zlouporabi.

4.5.7 Zaključak o nužnosti i proporcionalnosti predviđenih mjera

74. Kad je riječ o nužnosti i proporcionalnosti predviđenih mjera za otkrivanje, EDPB i EDPS posebno su zabrinuti zbog mjera predviđenih za otkrivanje nepoznatog materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece (vrbovanje) zbog njihova narušavanja privatnosti zbog mogućeg općeg odobravanja pristupa sadržaju komunikacija, njihove probabilističke prirode i stopa pogrešaka povezanih s takvim tehnologijama.
75. Nadalje, iz sudske prakse Suda EU-a može se zaključiti da je vjerojatnije da će mjere kojima se javnim tijelima omogućuje opći pristup sadržaju komunikacije utjecati na bit prava zajamčenih člancima 7. i 8. Povelje. Ta su razmatranja posebno relevantna u pogledu mjera za otkrivanje mamljenja djece predviđenih Prijedlogom.
76. U svakom slučaju, EDPB i EDPS smatraju da zadiranje do kojeg osobito dolazi zbog mjera za otkrivanje mamljenja djece nadilazi ono što je strogo nužno i razmjerno. Stoga bi te mjere trebalo ukloniti iz Prijedloga.

4.6 Obveze prijavljivanja

77. EDPB i EDPS preporučuju da se popis posebnih zahtjeva za prijavljivanje iz članka 13. Prijedloga nadopuni zahtjevom da se u prijavu uvrste informacije o konkretnoj tehnologiji koja je pružatelj usluga omogućila da postane svjestan relevantnog uvredljivog sadržaja, u slučaju da pružatelj usluga postane svjestan mogućeg seksualnog zlostavljanja djece nakon primjene mjera poduzetih za izvršavanje naloga za otkrivanje u skladu s člankom 7. Prijedloga.

4.7 Obveze uklanjanja i sprečavanja pristupa

78. Jedna od mjera predviđenih Prijedlogom za smanjenje rizika od širenja materijala koji sadržava seksualno zlostavljanje djece jest izdavanje naloga za uklanjanje i sprečavanje pristupa kojim bi se pružatelje usluga obvezalo na uklanjanje materijala koji sadržava seksualno zlostavljanje djece na internetu ili onemogućavanje ili sprečavanje pristupa takvom materijalu.⁶²
79. Iako je učinak naloga za uklanjanje na zaštitu podataka i privatnost komunikacija relativno ograničen, EDPB i EDPS podsjećaju na opće načelo koje treba poštovati, a to je da bi svaka mjera trebala biti što usmjerenija.

⁵⁹ Izvješće o procjeni učinka, Prilog 8., str. 281.–283.

⁶⁰ str. 15.–18.

⁶¹ Vidjeti prethodno točku 40.

⁶² Prijedlog, članci 14. i 16.

80. EDPB i EDPS istodobno skreću pozornost na činjenicu da pružatelji usluga pristupa internetu imaju pristup samo točnom URL-u sadržaja ako je taj sadržaj dostupan u obliku čistog teksta. Svaki put kad se sadržaj učini dostupnim putem HTTPS-a, pružatelj usluga pristupa internetu neće imati pristup točnom URL-u, osim ako ne dešifrira komunikaciju. Stoga EDPB i EDPS izražavaju sumnje u pogledu djelotvornosti mjera sprečavanja pristupa i smatraju da bi bilo nerazmjerno zahtijevati od pružatelja internetskih usluga da dešifriraju internetsku komunikaciju kako bi se spriječio pristup komunikacijama koje se odnose na materijal koji sadržava seksualno zlostavljanje djece.
81. Osim toga, općenitije gledano, treba napomenuti da je sprečavanje (ili onemogućavanje) pristupa digitalnoj stavci postupak koji se odvija na razini mreže i njegova se provedba može pokazati nedjelotvornom u slučaju višestrukih (sličnih, ali ne identičnih) primjeraka iste stavke. Nadalje, takav se postupak može pokazati nerazmjernim ako sprečavanje pristupa utječe na druge digitalne stavke koje nisu nezakonite kada su pohranjene na istom poslužitelju koji je nedostupan s pomoću mrežnih naredbi (npr. IP adresa ili stavljanje na crnu listu DNS-a). Osim toga, nisu svi načini sprečavanja pristupa na razini mreže jednako djelotvorni, a neke se može jednostavno izbjeći primjenom prilično jednostavnih tehničkih vještina.
82. Naposljetku, u predloženoj uredbi trebalo bi pojasniti ovlasti koordinacijskih tijela u pogledu izdavanja naloga za sprečavanje pristupa. Na primjer, na temelju trenutnog teksta članka 16. stavka 1. i članka 17. stavka 1. nije jasno jesu li koordinacijska tijela ovlaštena za izdavanje ili samo za zahtijevanje izdavanja naloga za sprečavanje pristupa.⁶³

4.8 Relevantne tehnologije i zaštitne mjere

4.8.1 Tehnička i integrirana zaštita podataka

83. Zahtjevi iz Prijedloga koji se primjenjuju na tehnologije koje bi trebalo uvesti za otkrivanje materijala koji sadržava seksualno zlostavljanje djece i mamljenja djece ne čine se dovoljno strogima. Konkretno, EDPB i EDPS napominju da se, suprotno analognim odredbama Privremene uredbe⁶⁴, u Prijedlogu ne upućuje izričito na načelo tehničke i integrirane zaštite podataka te se ne predviđa da tehnologije koje se upotrebljavaju za pregled teksta u komunikacijama ne smiju omogućivati donošenje zaključka o sadržaju komunikacija. U članku 10. stavku 3. točki (b) Prijedloga predviđa se samo da tehnologije ne smiju imati sposobnost „izdvajanja” nikakvih drugih informacija iz relevantnih komunikacija osim informacija koje su neophodne za otkrivanje. Međutim, čini se da taj standard nije dovoljno strog jer bi se o drugim informacijama mogao *donijeti zaključak* iz sadržaja komunikacije *bez izdvajanja* informacija kao takvih.
84. Stoga EDPS i EDPB preporučuju da se u Prijedlog uvede uvodna izjava u kojoj se navodi da se načelo tehničke i integrirane zaštite podataka utvrđeno u članku 25. Uredbe (EU) 2016/679 primjenjuje na tehnologije regulirane člankom 10. Prijedloga na temelju zakona te da se stoga ne treba ponavljati u pravnom tekstu. Osim toga, trebalo bi izmijeniti članak 10. stavak 3. točku (b) kako bi se osiguralo ne

⁶³ Članak 16. stavak 1. Prijedloga glasi: „Koordinacijsko tijelo u državi poslovnog nastana ovlašteno je zahtijevati od nadležnog pravosudnog tijela države članice koja ga je imenovala ili od neovisnog upravnog tijela te države članice da izda nalog za sprečavanje pristupa [...]”, dok članak 17. stavak 1. glasi „Koordinacijsko tijelo u državi poslovnog nastana izdaje naloge za sprečavanje pristupa iz članka 16. [...]” (isticanje dodano).

⁶⁴ Privremena uredba, članak 3. stavak 1. točka (b).

samo da ne omogućuju izdvajanje drugih informacija, nego i da ne omogućuju donošenje zaključka, kako je trenutačno predviđeno člankom 3. stavkom 1. točkom (b) Privremene uredbe.

4.8.2 Pouzdanost tehnologija

85. U Prijedlogu se pretpostavlja da pružatelju usluga mogu upotrebljavati nekoliko vrsta tehnoloških rješenja za izvršavanje naloga za otkrivanje. Konkretno, u Prijedlogu se pretpostavlja da su sustavi umjetne inteligencije dostupni i funkcioniraju za otkrivanje nepoznatog materijala koji sadržava seksualno zlostavljanje djece i otkrivanje mamljenja djece⁶⁵ te bi ih neka koordinacijska tijela mogla smatrati najsvremenijom tehnologijom. Iako djelotvornost Prijedloga ovisi o pouzdanosti tih tehnoloških rješenja, dostupno je vrlo malo informacija o općoj i sustavnoj primjeni tih tehnika, što zahtijeva pažljivo razmatranje.
86. Osim toga, iako su ih EDPB i EDPS morali upotrijebiti u svojoj procjeni proporcionalnosti zbog nedostatka alternativnih rješenja, treba napomenuti da pokazatelji uspješnosti tehnologija za otkrivanje navedeni u Izvješću o procjeni učinka priloženom Prijedlogu pružaju vrlo malo informacija o tome kako su procijenjeni i odražavaju li stvarnu učinkovitost relevantnih tehnologija. Ne postoje informacije o ispitivanjima ili referentnim vrijednostima koje dobavljači tehnologije upotrebljavaju za mjerenje te uspješnosti. Bez takvih informacija nije moguće ponoviti ispitivanja ili ocijeniti valjanost izvješća o uspješnosti. U tom pogledu treba napomenuti da bi, iako bi se pokazatelji uspješnosti mogli tumačiti kao da upućuju na to da neki alati za otkrivanje imaju visoku razinu točnosti (na primjer, točnost određenih alata za otkrivanje vrbovanja iznosi 88 %)⁶⁶, te bi pokazatelje trebalo razmotriti s obzirom na predviđenu praktičnu primjenu alata za otkrivanje, kao i ozbiljnost rizika koje bi pogrešna procjena određenog materijala podrazumijevala za relevantne ispitanike. Nadalje, EDPB i EDPS smatraju da, s obzirom na tako visokorizičnu obradu, stopa neuspjeha od 12 % predstavlja visok rizik za ispitanike koji su bili predmet lažno pozitivnih rezultata, čak i ako postoje zaštitne mjere za sprečavanje lažnih prijava tijelima za izvršavanje zakonodavstva. Malo je vjerojatno da bi pružatelji usluga mogli izdvojiti dovoljno sredstava za preispitivanje takvih lažno pozitivnih rezultata.
87. Kako je prethodno navedeno⁶⁷, pokazatelji uspješnosti trebali bi pružiti iscrpan uvid u ponašanje alata za otkrivanje. Kada se na slikama ili tekstu upotrebljavaju algoritmi umjetne inteligencije, postoje brojni dokazi da, zbog nedostatka zastupljenosti određenih skupina stanovništva u podacima koji se upotrebljavaju za učenje algoritma, može doći do predrasuda i diskriminacije. Te bi pristranosti trebalo utvrditi, izmjeriti i smanjiti na prihvatljivu razinu kako bi sustavi za otkrivanje bili istinski korisni za društvo u cjelini.
88. Iako je provedena studija o tehnologijama koje se upotrebljavaju za otkrivanje⁶⁸, EDPB i EDPS smatraju da je potrebna daljnja analiza kako bi se neovisno procijenila pouzdanost postojećih alata u stvarnim slučajevima upotrebe. Ta bi se analiza trebala temeljiti na iscrpnim pokazateljima uspješnosti i procijeniti učinak mogućih pogrešaka u uvjetima stvarnog života za sve ispitanike obuhvaćene Prijedlogom. Budući da su te tehnologije osnova na kojoj se temelji Prijedlog, EDPB i EDPS smatraju da je ta analiza od ključne važnosti za procjenu primjerenosti Prijedloga.
89. EDPB i EDPS ujedno napominju da se u Prijedlogu ne definiraju zahtjevi specifični za tehnologiju, ni u pogledu stope pogreške, ni u pogledu upotrebe klasifikatora i njihove provjere ili drugih ograničenja.

⁶⁵ Vidjeti Izvješće o procjeni učinka, str. 281.-282.

⁶⁶ Ibid., str. 283.

⁶⁷ Vidjeti prethodne točke 63.-64.

⁶⁸ Vidjeti Izvješće o procjeni učinka, str. 279. i dalje.

Zbog toga je te kriterije potrebno razviti u praksi pri procjeni proporcionalnosti primjene određene tehnologije, što dodatno pridonosi nedostatku točnosti i jasnoće.

90. S obzirom na posljedice za ispitanike u slučajevima lažno pozitivnih rezultata, EDPB i EDPS smatraju da se stope lažno pozitivnih rezultata moraju svesti na najmanju moguću mjeru i da te sustave treba osmisliti imajući na umu da velika većina elektroničkih komunikacija ne uključuje materijal koji sadržava seksualno zlostavljanje djece ni mamljenje djece te da će čak i vrlo niska stopa lažno pozitivnih rezultata podrazumijevati vrlo velik broj lažno pozitivnih rezultata s obzirom na količinu podataka koja će biti podvrgnuta otkrivanju. Općenito, EDPB i EDPS zabrinjava i činjenica da uspješnost dostupnih alata navedenih u Izvješću o procjeni učinka ne odražava precizne i usporedive pokazatelje u pogledu stopa lažno pozitivnih i lažno negativnih rezultata te smatraju da bi trebalo utvrditi usporedive i smislene pokazatelje uspješnosti za te tehnologije prije nego što ih se može smatrati dostupnima i učinkovitima.

4.8.3 Pregled audiokomunikacija

91. Za razliku od Privremene uredbe⁶⁹, Prijedlog iz svojeg područja primjene ne isključuje pregled audiokomunikacija u kontekstu otkrivanja mamljenja.⁷⁰ EDPB i EDPS smatraju da pregled audiokomunikacija posebno narušava privatnost jer bi to zahtijevalo aktivno, stalno i „uživo“ presretanje. Osim toga, u nekim državama članicama privatnost izgovorenih riječi uživa posebnu zaštitu.⁷¹ Nadalje, zbog činjenice da bi u načelu trebalo analizirati sav sadržaj audiokomunikacije, ova će mjera vjerojatno utjecati na bit prava zajamčenih člancima 7. i 8. Povelje. Stoga bi ova metoda otkrivanja trebala ostati izvan područja primjene obveza otkrivanja utvrđenih u predloženoj uredbi, i u pogledu glasovnih poruka i u pogledu komunikacije uživo, tim više s obzirom na činjenicu da u Izvješću o procjeni učinka koje je priloženo Prijedlogu nisu utvrđeni posebni rizici ili promjene u okruženju prijetnji koje bi opravdale njezinu upotrebu.⁷²

4.8.4 Provjera dobi

92. Prijedlogom se pružatelje usluga potiče na primjenu mjera za provjeru dobi i procjenu dobi kako bi se identificirala djeca korisnici njihovih usluga.⁷³ U tom pogledu EDPB i EDPS napominju da trenutačno ne postoji tehnološko rješenje kojim bi se sa sigurnošću mogla procijeniti dob korisnika u kontekstu interneta, bez oslanjanja na službeni digitalni identitet koji u ovoj fazi nije dostupan svakom europskom građaninu.⁷⁴ Stoga bi upotreba mjera za provjeru dobi predviđena u Prijedlogu mogla dovesti do isključivanja, npr., odraslih osoba koje izgledaju mlado iz pristupa internetskim uslugama ili do uvođenja alata za provjeru dobi koji uvelike narušavaju privatnost, što bi moglo spriječiti ili obeshrabrati legitimnu upotrebu predmetnih usluga.
93. U tom pogledu, iako se u uvodnoj izjavi 16. Prijedloga alati za roditeljsku kontrolu smatraju mogućim mjerama za smanjenje rizika, EDPB i EDPS preporučuju da se predložena uredba izmijeni kako bi se

⁶⁹ Usp. Privremenu uredbu, članak 1. stavak 2.

⁷⁰ Usp. Prijedlog, članak 1.

⁷¹ Vidjeti npr. njemački Kazneni zakon, odjeljak 201.

⁷² Vidjeti Izvješće o procjeni učinka.

⁷³ Vidjeti Prijedlog, članak 4. stavak 3., članak 6. stavak 1. točku (c) i uvodnu izjavu 16.

⁷⁴ Vidjeti npr. CNIL, 7. preporuka: Provjerite dob djeteta i pristanak roditelja uz poštovanje djetetove privatnosti (9. kolovoza 2021.)

pružateljima usluga izričito omogućilo da se, uz provjeru dobi ili kao njezina alternativa, oslanjaju na mehanizme za roditeljsku kontrolu.

4.9 Čuvanje informacija

94. Člankom 22. Prijedloga ograničavaju se svrhe u koje pružatelji usluga na koje se Prijedlog odnosi mogu zadržati podatke o sadržaju i druge podatke koji se obrađuju u vezi s mjerama koje se poduzimaju kako bi se ispunile obveze utvrđene u Prijedlogu. Međutim, u Prijedlogu se navodi da pružatelji usluga te informacije mogu čuvati i u svrhu poboljšanja djelotvornosti i točnosti tehnologija za otkrivanje seksualnog zlostavljanja djece na internetu radi izvršavanja naloga za otkrivanje, ali ne smiju pohranjivati osobne podatke u tu svrhu.⁷⁵
95. EDPB i EDPS smatraju da bi se zadržavanje podataka radi poboljšanja djelotvornosti i točnosti tehnologija trebalo dopustiti samo onim pružateljima usluga koji upotrebljavaju vlastite tehnologije za otkrivanje, dok se onima koji upotrebljavaju tehnologije koje pruža EU-ov centar ne bi smjela dopustiti ta mogućnost. Nadalje, EDPB i EDPS napominju da bi u praksi moglo biti teško osigurati da se osobni podatci ne pohranjuju u tu svrhu jer će većina podataka o sadržaju i drugih podataka koji se obrađuju u svrhu otkrivanja vjerojatno biti osobni podatci.

4.10 Učinak na šifriranje

96. Europska tijela za zaštitu podataka dosljedno se zalažu za široku dostupnost jakih alata za šifriranje i protiv svih oblika neovlaštenog pristupa („stražnjih vrata”).⁷⁶ Razlog je tome važnost šifriranja za osiguravanje ostvarivanja svih ljudskih prava na internetu i izvan njega.⁷⁷ Nadalje, tehnologije šifriranja bitno pridonose poštovanju privatnog života i povjerljivosti komunikacija te inovacijama i rastu digitalnog gospodarstva, koje se temelji na visokoj razini povjerenja i pouzdanosti koje takve tehnologije pružaju.
97. U kontekstu interpersonalnih komunikacija prolazno šifriranje („E2EE”) ključno je sredstvo za osiguravanje povjerljivosti elektroničkih komunikacija jer pruža snažne tehničke zaštitne mjere kojima se sprečava pristup sadržaju komunikacija svima osim pošiljatelju i primatelju, uključujući i pružatelju usluga. Sprečavanje ili odvratanje od uporabe E2EE-a, nametanje obveze pružateljima usluga da obrađuju elektroničke komunikacijske podatke u svrhe koje nisu pružanje njihovih usluga ili nametanje obveze proaktivnog prosljeđivanja elektroničke komunikacije trećim stranama dovelo bi do rizika da pružatelji usluga nude manje šifrirane usluge kako bi bolje ispunili obveze, čime bi se općenito oslabila uloga šifriranja i narušilo poštovanje temeljnih prava europskih građana. Treba napomenuti da, iako je E2EE jedna od najčešće upotrebljivanih sigurnosnih mjera u kontekstu elektroničkih komunikacija, druga tehnička rješenja (npr. upotreba drugih kriptografskih shema) mogu biti ili postati jednako važna za osiguravanje i zaštitu povjerljivosti digitalnih komunikacija. Stoga njihovu primjenu ne bi trebalo sprečavati ili obeshrabrivati.

⁷⁵ Prijedlog, članak 22. stavak 1.

⁷⁶ Vidjeti npr. članak 29. Izjave Radne skupine za zaštitu podataka o šifriranju i njihovu utjecaju na zaštitu pojedinaca u pogledu obrade njihovih osobnih podataka u EU-u (11. travnja 2018.).

⁷⁷ Vidjeti Rezoluciju 47/16 Vijeća za ljudska prava o promicanju, zaštiti i uživanju ljudskih prava na internetu, dokument UN-a A/HRC/RES/47/16 (26. srpnja 2021.).

98. Uvođenje alata za presretanje i analizu interpersonalnih elektroničkih komunikacija u osnovi je u suprotnosti s E2EE-om jer se potonjim nastoji tehnički zajamčiti povjerljivost komunikacije između pošiljatelja i primatelja.
99. Stoga, iako se Prijedlogom ne utvrđuje obveza sustavnog presretanja za pružatelje usluga, sama mogućnost izdavanja naloga za otkrivanje vjerojatno će znatno opteretiti odluke pružatelja usluga u pogledu tehničkih rješenja, osobito s obzirom na ograničeni vremenski okvir za postupanje u skladu s takvim nalogom i visoke kazne s kojima bi se suočili u slučaju da to ne učine.⁷⁸ To bi u praksi moglo dovesti do toga da će određeni pružatelji usluga prestati upotrebljavati E2EE.
100. Potrebno je na odgovarajući način procijeniti učinak koji može proizaći iz Prijedloga u smislu slabljenja upotrebe E2EE-a ili odvrćanja od nje. Svakom od tehnika za izbjegavanje zaštite privatnosti E2EE-a koje su predstavljene u Izvješću o procjeni učinka priloženom Prijedlogu uveli bi se sigurnosni nedostaci.⁷⁹ Na primjer, pregled na strani klijenta⁸⁰ vjerojatno bi doveo do značajnog, neusmjerenog pristupa i obrade nešifriranog sadržaja na uređajima krajnjeg korisnika. Takvo značajno narušavanje povjerljivosti posebno bi utjecalo na djecu jer je vjerojatnije da će usluge kojima se oni koriste biti obuhvaćene nalogima za otkrivanje, zbog čega će djeca biti izložena praćenju ili prisluškivanju. Istodobno, pregled *na strani poslužitelja* također je u osnovi nespojiv s paradigmom E2EE jer bi trebalo prekinuti komunikacijski kanal, šifriran na krajnjim točkama, što će dovesti do masovne obrade osobnih podataka na poslužiteljima pružatelja usluga.
101. Iako se u Prijedlogu navodi da se „predmetnom pružatelju prepušta odabir tehnologija koje će upotrebljavati za učinkovito izvršavanje naloga za otkrivanje i to se ne bi trebalo tumačiti kao poticanje ili odvrćanje od upotrebe bilo koje određene tehnologije”⁸¹, strukturna neusklađenost određenog naloga za otkrivanje s E2EE-om snažno odvrća od upotrebe E2EE-a. Nemogućnost pristupa uslugama koje upotrebljavaju E2EE (koje su trenutačna najnovija dostignuća u smislu tehničkog jamstva povjerljivosti) i njihove upotrebe mogla bi imati odvrćajući učinak na slobodu izražavanja i legitimnu privatnu upotrebu elektroničkih komunikacijskih usluga. Komisija je prepoznala negativan odnos otkrivanja materijala koji sadržava seksualno zlostavljanje djece ili mamljenje djece i E2EE-a kada je u Izvješću o procjeni učinka⁸² navela vjerojatnost da će uvođenje sustava E2EE u Facebooku 2023. dovesti do okončanja dobrovoljnog pregleda Facebooka.
102. Kako bi se osiguralo da se predloženom uredbom ne ugrožava sigurnost ili povjerljivost elektroničkih komunikacija europskih građana, EDPB i EDPS smatraju da bi u normativnom dijelu Prijedloga trebalo jasno navesti da se ništa u predloženoj uredbi ne bi smjelo tumačiti kao zabranu ili slabljenje šifriranja, u skladu s onime što je navedeno u uvodnoj izjavi 25. Privremene uredbe.

⁷⁸ Usp. Prijedlog, članak 35.

⁷⁹ Vidjeti odjeljak 4.2 u Abelson, Harold, Ross J. Anderson, Steven M. Bell ovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague i Carmela Troncoso, „Bugs in our Pockets: The Risks of Client-S side Scanning”, arXiv abs/2110.07450 (2021.).

⁸⁰ Pregled na strani klijenta općenito se odnosi na sustave koji pregledavaju sadržaje poruka radi podudaranja s bazom podataka upitnog sadržaja prije nego što se poruka pošalje predviđenom primatelju.

⁸¹ Prijedlog, uvodna izjava 26.

⁸² Izvješće o procjeni učinka, str. 27.

4.11 Nadzor, provedba i suradnja

4.11.1 Uloga nacionalnih nadzornih tijela u skladu s Općom uredbom o zaštiti podataka

103. Prijedlogom se predviđa uspostava mreže nacionalnih koordinacijskih tijela koja će biti odgovorna za primjenu i provedbu predložene uredbe.⁸³ Iako se u uvodnoj izjavi 45. Prijedloga navodi da „pravila ove Uredbe o nadzoru i provedbi ne bi se trebala tumačiti na način da utječu na ovlasti i nadležnosti tijela za zaštitu podataka u skladu s Uredbom (EU) 2016/679”, EDPB i EDPS smatraju da bi trebalo bolje urediti odnos između zadaća koordinacijskih tijela i zadaća tijela za zaštitu podataka te da bi se tijelima za zaštitu podataka trebala dati istaknutija uloga u okviru predložene uredbe.
104. Konkretno, od pružatelja usluga trebalo bi se zahtijevati da se savjetuju s tijelima za zaštitu podataka u sklopu postupka prethodnog savjetovanja kako je navedeno u članku 36. Opće uredbe o zaštiti podataka prije uvođenja bilo kojih mjera za otkrivanje materijala koji sadržava seksualno zlostavljanje djece ili mamljenja, a ne isključivo u vezi s primjenom mjera za otkrivanje mamljenja djece, kako je trenutačno predviđeno Prijedlogom.⁸⁴ Trebalo bi smatrati da sve mjere za otkrivanje automatski dovode do „visokog rizika” te bi stoga trebale proći postupak prethodnog savjetovanja bez obzira na to odnose li se na vrbovanje ili materijal koji sadržava seksualno zlostavljanje djece, kao što je već slučaj u okviru Privremene uredbe.⁸⁵ Osim toga, nadležna tijela za zaštitu podataka imenovana na temelju Opće uredbe o zaštiti podataka trebala bi uvijek imati ovlast za iznošenje svojih stajališta o predviđenim mjerama za otkrivanje, a ne samo u posebnim okolnostima.⁸⁶
105. Nadalje, predloženom uredbom trebalo bi uspostaviti sustav za rješavanje sporova između nadležnih tijela i tijela za zaštitu podataka u vezi s nalogima za otkrivanje. Konkretno, tijela za zaštitu podataka trebala bi imati pravo osporiti nalog za otkrivanje pred sudovima države članice nadležnog pravosudnog tijela ili neovisnog upravnog tijela koje je izdalo nalog za otkrivanje. U tom pogledu EDPB i EDPS napominju da, u skladu s trenutačnom verzijom Prijedloga, nadležno tijelo može odbaciti mišljenje nadležnih tijela za zaštitu podataka pri izdavanju naloga za otkrivanje. To bi moglo dovesti do proturječnih odluka jer bi tijela za zaštitu podataka, kako je potvrđeno člankom 36. stavkom 2. Opće uredbe o zaštiti podataka, zadržala cijeli niz svojih korektivnih ovlasti u skladu s člankom 58. Opće uredbe o zaštiti podataka, uključujući ovlast izdavanja naloga za zabranu obrade.

4.11.2 Uloga EDPB-a

106. EDPB i EDPS napominju da se Prijedlogom u članku 50. stavku 1. trećoj rečenici predviđa da „EU-ov centar traži mišljenje svog Tehnološkog odbora i Europskog odbora za zaštitu podataka” prije nego što određenu tehnologiju uvrsti na popise tehnologija koje pružatelji usluga smještaja informacija na poslužitelju i pružatelji interpersonalnih komunikacijskih usluga mogu razmotriti za izvršavanje naloga za otkrivanje. Predviđa se i da EDPB svoja mišljenja dostavlja u roku od osam tjedana, a taj se rok prema potrebi može produljiti za dodatnih šest tjedana, uzimajući u obzir složenost predmeta. Naposljetku se od EDPB-a zahtijeva da o bilo kojem takvom produljenju obavijesti EU-ov centar u roku od mjesec dana od zaprimanja zahtjeva za savjetovanje, zajedno s razlozima odgode.

⁸³ Prijedlog, članak 25.

⁸⁴ Prijedlog, članak 7. stavak 3. druga alineja točka (b).

⁸⁵ Privremena uredba, članak 3. stavak 1. točka (c).

⁸⁶ Us p. Prijedlog, članak 7. stavak 3. druga alineja točka (c).

107. Postojeće zadaće EDPB-a utvrđene su u članku 70. Opće uredbe o zaštiti podataka i članku 51. Direktive (EU) 2016/680 (u nastavku „LED”)⁸⁷. Predviđeno je da će u okviru tih zadaća EDPB pružati savjete Komisiji i davati mišljenja na zahtjev Komisije, nacionalnog nadzornog tijela ili njegova predsjednika. Iako se u članku 1. stavku 3. točki (d) Prijedloga navodi da Prijedlog neće imati učinak na pravila utvrđena u Općoj uredbi o zaštiti podataka i LED-u, davanje ovlasti EU-ovu centru da traži mišljenja EDPB-a nadilazi zadaće dodijeljene EDPB-u na temelju Opće uredbe o zaštiti podataka i LED-a. Stoga bi u predloženoj uredbi, barem u uvodnoj izjavi, trebalo pojasniti da se Prijedlogom proširuju zadaće EDPB-a. U tom pogledu EDPB i EDPS cijene važnu ulogu koju Prijedlog dodjeljuje EDPB-u zahtijevajući njegovo sudjelovanje u praktičnoj provedbi predložene uredbe. Tajništvo EDPB-a u praksi ima ključnu ulogu u pružanju analitičke, administrativne i logističke potpore potrebne za donošenje mišljenja EDPB-a. Stoga je, kako bi se osiguralo da EDPB i njegovi članovi mogu ispuniti svoje zadaće, nužno EDPB-u dodijeliti dostatna proračunska sredstva i osoblje. Nažalost, u zakonodavnom financijskom izvještaju Prijedloga ne navodi se da će se na raspolaganje staviti dodatna sredstva za obavljanje dodatnih zadaća koje se prijedlogom dodjeljuju EDPB-u.⁸⁸
108. Nadalje, EDPB i EDPS napominju da se u članku 50. Prijedloga ne navodi kako će EU-ov centar postupiti nakon što primi mišljenje EDPB-a.⁸⁹ U uvodnoj izjavi 27. Prijedloga navodi se samo da EU-ov centar i Europska komisija trebaju uzeti u obzir savjet EDPB-a. Stoga bi trebalo pojasniti koju će svrhu zatraženo mišljenje imati u postupku iz članka 50. Prijedloga i kako bi EU-ov centar trebao postupiti nakon što dobije mišljenje EDPB-a.
109. Osim toga, EDPB i EDPS smatraju da će, iako će se EDPB-ovim smjernicama ili mogućim mišljenjem o upotrebi tehnologija za otkrivanje ocijeniti upotreba takvih tehnologija na općoj razini, nacionalno nadzorno tijelo za prethodno savjetovanje na temelju članka 36. Opće uredbe o zaštiti podataka trebati uzeti u obzir posebne okolnosti i provesti procjenu namjeravane obrade koju provodi relevantni voditelj obrade za svaki pojedinačni slučaj. EDPB i EDPS napominju da će nadzorna tijela primjenjivati i da bi trebala primjenjivati kriterije utvrđene u članku 36. Opće uredbe o zaštiti podataka kako bi odlučila je li potrebno produljiti rok utvrđen u Općoj uredbi o zaštiti podataka za davanje njihova mišljenja kao odgovor na prethodno savjetovanje te da nema potrebe za primjenom različitih standarda kad se prethodno savjetovanje odnosi na primjenu tehnologije za otkrivanje.⁹⁰
110. Naposljetku, u primjeni članka 11. („Smjernice u pogledu obveza otkrivanja”) Prijedlogom se propisuje da Komisija može izdati smjernice o primjeni članaka od 7. do 10. Prijedloga. Članak 11. Prijedloga trebalo bi izmijeniti kako bi se pojasnilo da bi se Komisija, uz koordinacijska tijela i EU-ov centar, trebala savjetovati i s EDPB-om o nacrtu smjernica izvan predviđenog postupka javnog savjetovanja prije izdavanja smjernica o obvezama otkrivanja.
111. Stoga je za tu zadaću EDPB-a i njegovu ulogu unutar pravnog okvira koji će biti uveden Prijedlogom potrebna daljnja procjena zakonodavca.

⁸⁷ Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvansnagne Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89. – 131.).

⁸⁸ Us p. Prijedlog, str. 105. i dalje

⁸⁹ Vidjeti, usporedbe radi, članak 51. stavak 4. LED-a.

⁹⁰ Us p. Prijedlog, uvodna izjava 24.

4.11.3 Uloga EU-ova centra za seksualno zlostavljanje djece

112. Poglavljem IV. Prijedloga uspostavio bi se EU-ov centar kao nova decentralizirana agencija kojom će se omogućiti provedba Prijedloga. Među ostalim zadaćama, EU-ov centar trebao bi pružateljima usluga olakšati pristup pouzdanim tehnologijama za otkrivanje; staviti na raspolaganje dostupne pokazatelje stvorene na temelju seksualnog zlostavljanja djece na internetu koje su provjerili sudovi ili neovisna upravna tijela država članica u svrhu otkrivanja; na zahtjev, pružiti određenu pomoć za provedbu procjena rizika; i pružiti potporu u komunikaciji s relevantnim nacionalnim tijelima.⁹¹
113. U tom pogledu EDPB i EDPS pozdravljaju članak 77. stavak 1. Prijedloga kojim se potvrđuje da obrada osobnih podataka koju provodi EU-ov centar podliježe EUDPR-u te se predviđa da se mjere za primjenu te Uredbe od strane EU-ova centra, uključujući one koje se odnose na imenovanje službenika EU-ova centra za zaštitu podataka, utvrđuju nakon savjetovanja s EDPS-om. Međutim, EDPB i EDPS smatraju da je potrebno pomnije razmotriti nekoliko odredbi ovog poglavlja.
114. Kao prvo, EDPB i EDPS napominju da se u članku 48. Prijedloga propisuje prosljeđivanje svih prijava koje „nisu očito neutemeljene”⁹² nacionalnim tijelima za izvršavanje zakonodavstva i Agenciji EU-a za suradnju tijela za izvršavanje zakonodavstva („Europol”). Taj se prag za prosljeđivanje prijava iz EU-ova centra nacionalnim tijelima za izvršavanje zakonodavstva i Europolu (koje „nisu očito neutemeljene”) čini preniskim, osobito imajući na umu da je svrha uspostave EU-ova centra, kako je navedeno u Komisijinom Izvješću o procjeni učinka⁹³, smanjiti opterećenje tijela za izvršavanje zakonodavstva i Europolu u vezi s filtriranjem sadržaja pogrešno označenog kao materijal koji sadržava seksualno zlostavljanje djece. U tom pogledu nije jasno zašto EU-ov centar, kao središte stručnog znanja, ne bi mogao provesti detaljniju i činjeničnu procjenu kako bi se ograničio rizik od prijenosa podataka nedužnih osoba tijelima za izvršavanje zakonodavstva.
115. Kao drugo, odredba koja se odnosi na trajanje pohrane osobnih podataka koju provodi EU-ov centar čini se relativno fleksibilnom s obzirom na osjetljivost predmetnih podataka. Čak i ako ne bi bilo moguće odrediti najdulje razdoblje za čuvanje tih podataka, EDPB i EDPS preporučuju da se u Prijedlogu utvrdi barem najdulji rok za preispitivanje potrebe za daljnjom pohranom podataka i zahtijevanje obrazloženja za produljeno zadržavanje podataka nakon tog razdoblja.
116. Osim toga, s obzirom na vrlo veliku osjetljivost osobnih podataka koje će obrađivati EU-ov centar, EDPB i EDPS smatraju da bi obrada trebala podlijegati dodatnim zaštitnim mjerama, osobito kako bi se osigurao djelotvoran nadzor. To bi moglo uključivati obvezu EU-ova centra da vodi evidenciju za postupke obrade u automatiziranim sustavima obrade podataka (tj. u skladu sa zahtjevima u pogledu operativnih osobnih podataka iz poglavlja IX. EUDPR-a), uključujući evidentiranje unosa, izmjene, pristupanja, uvida, otkrivanja, kombiniranja i brisanja osobnih podataka. Evidencije o obavljanju uvida i otkrivanju podataka omogućuju da se ustanovi razlog, datum i vrijeme takvih postupaka, identitet osobe koja je imala uvid u operativne osobne podatke ili ih je otkrila te, u mjeri u kojoj je to moguće, identitet primatelja. Ta bi se evidencija upotrebljavala za provjeru zakonitosti obrade, samopraćenja i

⁹¹ Vidjeti COM(2022) 209 final, str. 7.

⁹² Pojam „očito neutemeljen” opisan je u uvodnoj izjavi 65. Prijedloga kao slučajevi „u kojima je odmah očito, bez materijalne pravne ili činjenične analize, da prijavljene aktivnosti ne predstavljaju seksualno zlostavljanje djece na internetu”.

⁹³ Vidjeti, na primjer, stranicu 349. Izvješća o procjeni učinka.

za osiguravanje njezina integriteta i sigurnosti te bi se na zahtjev stavila na raspolaganje službeniku EU-ova centra za zaštitu podataka i EDPS-u.

117. Nadalje, u Prijedlogu se upućuje na obvezu pružatelja usluga da korisnike obavijeste o otkrivanju materijala koji sadržava seksualno zlostavljanje djece putem naloga za otkrivanje, kao i o pravu na podnošenje pritužbe koordinacijskom tijelu.⁹⁴ Međutim, Prijedlogom se ne utvrđuju postupci za ostvarivanje prava ispitanika, uzimajući u obzir i višestruke lokacije na kojima se osobni podatci mogu prenositi i pohranjivati u skladu s Prijedlogom (EU-ov centar, Europol, nacionalne agencije za izvršavanje zakonodavstva). Zahtjev za obavješćivanje korisnika trebao bi uključivati obvezu obavješćivanja pojedinaca da su njihovu podatci proslijeđeni i da ih obrađuju različiti subjekti, ako je primjenjivo (npr. nacionalne agencije za izvršavanje zakonodavstva i Europol). Osim toga, trebao bi postojati centralizirani postupak za primanje i koordinaciju zahtjeva za pravo na pristup, ispravak i brisanje ili, alternativno, obveza suradnje subjekta koji prima zahtjev ispitanika s drugim predmetnim subjektima.
118. EDPB i EDPS napominju da je u skladu s člankom 50 Prijedloga zadaća EU-ova centra utvrditi popis tehnologija koje se mogu upotrebljavati za izvršavanje naloga za otkrivanje. Međutim, u skladu s člankom 12. stavkom 1. Prijedloga obveza je pružatelja usluga prijaviti sve informacije koje upućuju na potencijalno seksualno zlostavljanje djece u okviru njihovih usluga, a ne samo one koje proizlaze iz izvršavanja naloga za otkrivanje. Vrlo je vjerojatno da bi znatna količina takvih informacija proizašla iz provedbe mjera za smanjenje rizika pružatelja usluga, u skladu s člankom 4. Prijedloga. Stoga se čini ključnim utvrditi što bi te mjere mogle biti, njihovu djelotvornost, njihovu stopu pogreške u prijavljivanju mogućeg seksualnog zlostavljanja djece te njihov učinak na prava i slobode pojedinaca. Unatoč činjenici da se u članku 4. stavku 5. Prijedloga navodi da Komisija, u suradnji s koordinacijskim tijelima i EU-ovim centrom te nakon javnog savjetovanja, može izdati relevantne smjernice, EDPB i EDPS smatraju da je važno da zakonodavac u članak 50. uključi i zadaću EU-ova centra da stavi na raspolaganje i popis preporučenih mjera za smanjenje rizika i relevantnih najboljih praksi koje su posebno djelotvorne u utvrđivanju mogućeg seksualnog zlostavljanja djece na internetu. Budući da takve mjere mogu zadirati u temeljna prava na zaštitu podataka i privatnost, preporučuje se i da EU-ov centar zatraži mišljenje EDPB-a prije objave takvog popisa.
119. Naposljetku, sigurnosni zahtjevi utvrđeni u članku 51. stavku 4. Prijedloga trebali bi biti konkretniji. U tom se pogledu može ravnati prema sigurnosnim zahtjevima utvrđenima u drugim uredbama o opsežnim sustavima koji uključuju visokorizičnu obradu, kao što su Uredba 767/2008⁹⁵ (vidjeti

⁹⁴ Vidjeti članak 10. stavak 6. i, nakon podnošenja prijave EU-ovu centru, članak 12. stavak 2. Prijedloga.

⁹⁵ Uredba (EZ) br. 767/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o viznom i informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak (Uredba o VIS-u), SLL 218, 13.8.2008., str. 60.–81.

članak 32.), Uredba 1987/2006⁹⁶ (vidjeti članak 16.), Uredba 2018/1862⁹⁷ (vidjeti članak 16.) i Uredba 603/2013⁹⁸ (vidjeti članak 34.).

4.11.4 Uloga Europolu

120. Prijedlogom se predviđa bliska suradnja EU-ova centra i Europolu. U skladu s poglavljem IV. Prijedloga, po primitku prijava pružatelja usluga o sumnji na materijal koji sadržava seksualno zlostavljanje djece, EU-ov centar ih provjerava kako bi procijenio koje su prijave provedive (nisu očito neutemeljene) i prosljeđuje ih Europolu te nacionalnim tijelima za izvršavanje zakonodavstva.⁹⁹ EU-ov centar Europolu odobrava pristup svojim bazama podataka pokazatelja i bazama podataka prijava kako bi se Europolu pomoglo u istragama navodnih kaznenih djela seksualnog zlostavljanja djece.¹⁰⁰ Nadalje, EU-ovu centru omogućio bi se „najpotpuniji” pristup informacijskim sustavima Europolu.¹⁰¹ Dvije agencije također će dijeliti poslovne prostore i određenu (neoperativnu) infrastrukturu.¹⁰²
121. EDPB i EDPS napominju da nekoliko aspekata povezanih sa suradnjom predloženog EU-ova centra i Europolu izaziva zabrinutost ili zahtijeva dodatne specifikacije.

O prosljeđivanju prijava iz EU-ova centra Europolu (članak 48.)

122. Člankom 48. predložene uredbe od EU-ova centra zahtijeva se da prijave koje se ne smatraju očito neutemeljenima, zajedno sa svim drugim dodatnim relevantnim informacijama, prosljedi Europolu i nadležnom tijelu ili tijelima za izvršavanje zakonodavstva država članica koja bi mogla biti nadležna za istragu ili kazneni progon mogućeg seksualnog zlostavljanja djece. Iako se ovim člankom Europolu dodjeljuje uloga utvrđivanja relevantnog tijela za izvršavanje zakonodavstva u slučaju nejasnoće u pogledu predmetne države članice, tom se odredbom zapravo predviđa da se sve prijave šalju Europolu bez obzira na to je li nacionalno tijelo utvrđeno i je li mu EU-ov centar već prenio prijavu.

⁹⁶ Uredba (EZ) br. 1987/2006 Europskog parlamenta i Vijeća od 20. prosinca 2006. o uspostavi, djelovanju i korištenju druge generacije Schengenskog informacijskog sustava (SIS II), (SL L 381, 28.12.2006., str. 4.–23.).

⁹⁷ Uredba (EU) 2018/1862 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, izmjeni i stavljanju izvan snage Odluke Vijeća 2007/533/PUP i stavljanju izvan snage Uredbe (EZ) br. 1986/2006 Europskog parlamenta i Vijeća i Odluke Komisije 2010/261/EU (SL L 312, 7.12.2018., str. 56.–106.).

⁹⁸ Uredba (EU) br. 603/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o uspostavi sustava „Eurodac” za usporedbu otisaka prstiju za učinkovitu primjenu Uredbe (EU) br. 604/2013 o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva i o zahtjevima za usporedbu s podacima iz Eurodaca od strane tijela kaznenog progona država članica i Europolu u svrhu kaznenog progona te o izmjeni Uredbe (EU) br. 1077/2011 o osnivanju Europske agencije za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde (SL L 180, 29.6.2013., str. 1.–30.).

⁹⁹ Vidjeti članak 48. Prijedloga.

¹⁰⁰ Vidjeti članak 4. stavke od 4. do 5. Prijedloga.

¹⁰¹ Vidjeti članak 53. stavak 2. Prijedloga.

¹⁰² Posebno u pogledu upravljanja ljudskim resursima, informacijske tehnologije (IT), uključujući kibersigurnost, zgrade i komunikacije.

123. Međutim, u Prijedlogu se ne pojašnjava što bi bila dodana vrijednost Europolova sudjelovanja ili njegove očekivane uloge po primitku prijave, osobito u onim slučajevima u kojima je nacionalno tijelo za izvršavanje zakonodavstva utvrđeno i istodobno je već obaviješteno.¹⁰³
124. EDPB i EDPS podsjećaju da je Europolov mandat ograničen na podupiranje djelovanja nadležnih tijela država članica i njihovu uzajamnu suradnju u sprečavanju i suzbijanju teških kaznenih djela koja utječu na dvije države članice ili više njih.¹⁰⁴ U članku 19. Uredbe (EU) 2106/794¹⁰⁵ kako je izmijenjena Uredbom (EU) 2022/991¹⁰⁶ („izmijenjena Uredba o Europolu“) propisuje se da je tijelo Unije koje Europolu dostavlja informacije obvezno utvrditi svrhu ili svrhe u koje ih Europol treba obrađivati te uvjete obrade. Odgovorno je i za osiguravanje točnosti osobnih podataka koji se prenose.¹⁰⁷
125. Općenito prosljeđivanje prijava Europolu bilo bi stoga u suprotnosti s izmijenjenom Uredbom o Europolu i podrazumijevalo bi niz rizika za zaštitu podataka. Udvostručavanje obrade osobnih podataka moglo bi dovesti do toga da se istovremeno paralelno pohranjuju višestruke kopije istih vrlo osjetljivih osobnih podataka (npr. u EU-ovu centru, Europolu, nacionalnom tijelu za izvršavanje zakonodavstva), uz rizike u pogledu točnosti podataka zbog moguće desinkronizacije baza podataka, kao i za ostvarivanje prava ispitanika. Nadalje, nizak prag utvrđen u Prijedlogu za dijeljenje prijava s tijelima za izvršavanje zakonodavstva (koje „nisu očito neutemeljene“) upućuje na veliku vjerojatnost da će lažni pozitivni rezultati (tj. sadržaj koji je greškom označen kao seksualno zlostavljanje djece) biti pohranjeni u informacijskim sustavima Europolu, moguće tijekom duljeg razdoblja.¹⁰⁸
126. EDPB i EDPS stoga preporučuju da se u Prijedlogu navedu i ograniče okolnosti i svrhe u kojima bi EU-ov centar mogao proslijediti prijave Europolu, u skladu s izmijenjenom Uredbom o Europolu. Time bi se trebale izričito isključiti one okolnosti u kojima su prijave proslijeđene tijelu za izvršavanje zakonodavstva relevantne države članice, koje ne podrazumijevaju prekograničnu dimenziju. Osim toga, Prijedlog bi trebao uključivati zahtjev da EU-ov centar prenosi Europolu samo osobne podatke koji su primjereni, relevantni i ograničeni na ono što je strogo nužno. Moraju se predvidjeti i posebne zaštitne mjere za osiguravanje kvalitete i pouzdanosti podataka.

¹⁰³ U uvodnoj i zjavi 71. Prijedloga samo se općenito upućuje na Europolovo iskustvo u utvrđivanju nadležnih nacionalnih tijela u nejasnim situacijama i njegovu bazu obavještajnih podataka koji mogu pridonijeti utvrđivanju poveznica s istragama u drugim državama članicama.

¹⁰⁴ Vidjeti članak 3. izmijenjene Uredbe o Europolu.

¹⁰⁵ Uredba (EU) 2016/794 Europskog parlamenta i Vijeća od 11. svibnja 2016. o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol) te zamjeni i stavljanju izvan snage odluka Vijeća 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP (SL L 135, 24.5.2016., str. 53.–114.).

¹⁰⁶ Uredba (EU) 2022/991 Europskog parlamenta i Vijeća od 8. lipnja 2022. o izmjeni Uredbe (EU) 2016/794 u pogledu suradnje Europolu s privatnim stranama, obrade osobnih podataka koju provodi Europol radi potpore kaznenim istragama i uloge Europolu u području istraživanja i inovacija (SL L 169, 27.6.2022., str. 1.–42.).

¹⁰⁷ Članak 38. stavak 2. točka (a) izmijenjene Uredbe o Europolu.

¹⁰⁸ Prema Komisijinu Izvješću o procjeni učinka, Europol je bio u mogućnosti ispitati samo 20 % od 50 milijuna jedinstvenih slika i videozapisa s materijalom koji sadržava seksualno zlostavljanje djece u svojoj bazi podataka, što upućuje na nedostatak resursa za mjere u vezi s materijalima koji sadržavaju seksualno zlostavljanje djece koje trenutačno prima. Vidjeti Izvješće o procjeni učinka priloženo Prijedlogu uredbe o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece, SWD(2022), str. 47.–48.

Članak 53. stavak 2. o suradnji EU-ova centra i Europol

127. Člankom 53. stavkom 2. Prijedloga zahtijeva se da si Europol i EU-ov centar međusobno daju „najpotpuniji pristup relevantnim informacijskim sustavima ako je to potrebno za obavljanje njihovih zadaća te u skladu s aktima prava Unije kojima se uređuje takav pristup”.
128. U članku 46. stavcima 4. i 5. Prijedloga dalje se navodi da će Europol imati pristup bazi podataka pokazatelja i bazi podataka prijava EU-ova centra, a u članku 46. stavku 6. utvrđuje se postupak za odobravanje tog pristupa: Europol podnosi zahtjev u kojem navodi svrhu i stupanj pristupa koji su potrebni za ispunjavanje te svrhe, a koji EU-ov centar temeljito ocjenjuje.
129. Kriteriji i zaštitne mjere kojima se uvjetuje Europolov pristup i naknadna upotreba podataka dobivenih iz informacijskih sustava EU-ova centra nisu navedeni. Nadalje, nije objašnjeno zašto je potrebno Europolu odobriti izravan pristup informacijskim sustavima agencije koja nije agencija za izvršavanje zakonodavstva, pri čemu ti sustavi sadržavaju vrlo osjetljive osobne podatke, čija povezanost s kaznenim djelima i sprečavanjem kaznenih djela možda nije utvrđena. Kako bi se osigurala visoka razina zaštite podataka i usklađenost s načelom ograničena svrhe, EDPB i EDPS preporučuju da se osobni podatci iz EU-ova centra Europolu prenose samo na pojedinačnoj osnovi, nakon temeljito procijenjenog zahtjeva, primjenom alata za sigurnu razmjenu komunikacije, kao što je SIENA¹⁰⁹.
130. Jedino upućivanje na pristup EU-ova centra informacijskim sustavima Europolu navedeno je u članku 53. stavku 2. Stoga nije jasno u koje bi svrhe i na temelju kojih posebnih zaštitnih mjera došlo do takvog pristupa.
131. EDPB i EDPS podsjećaju da je Europol agencija za izvršavanje zakonodavstva koja je uspostavljena u skladu s Ugovorima EU-a s osnovnom zadaćom za sprečavanje i suzbijanje teških kaznenih djela. Stoga operativni osobni podatci koje obrađuje Europol podliježu strogim pravilima i zaštitnim mjerama za obradu podataka. Predloženi EU-ov centar nije tijelo za izvršavanje zakonodavstva te mu ni u kojem slučaju ne bi trebalo odobriti pristup informacijskim sustavima Europolu.
132. EDPS i EDPB dalje napominju da će se velik dio informacija od zajedničkog interesa za EU-ov centar i Europol odnositi na osobne podatke žrtava navodnih kaznenih djela, osobne podatke maloljetnika i osobne podatke o seksualnom životu, koji se smatraju posebnim kategorijama osobnih podataka na temelju izmijenjene Uredbe o Europolu. Izmijenjenom Uredbom o Europolu uvode se strogi uvjeti u pogledu pristupa posebnim kategorijama osobnih podataka. Člankom 30. stavkom 3. izmijenjene Uredbe o Europolu propisuje se da samo Europol ima izravan pristup takvim osobnim podacima, točnije samo ograničen broj službenika Europolu koje propisno ovlasti izvršni direktor.¹¹⁰
133. EDPB i EDPS stoga preporučuju da se pojasni tekst članka 53. stavka 2. Prijedloga kako bi se na odgovarajući način uzela u obzir ograničenja na temelju izmijenjene Uredbe o Europolu i kako bi se utvrdili način pristupa EU-ova centra. Konkretno, svaki pristup osobnim podacima koji se obrađuju u informacijskim sustavima Europolu, ako se to smatra nužnim za obavljanje zadaća EU-ova centra, trebao bi se odobriti samo na pojedinačnoj osnovi, nakon podnošenja izričitog zahtjeva, kojim se dokumentiraju posebna svrha i uz obrazloženje. Od Europolu bi se trebalo zahtijevati da temeljito

¹⁰⁹ Mrežna aplikacija za sigurnu razmjenu i informacija (SIENA).

¹¹⁰ U skladu s izmijenjenom Uredbom o Europolu iznimke od te zabrane utvrđene su za agencije Unije osnovane na temelju glave V. UFEU-a. Međutim, s obzirom na pravnu osnovu Prijedloga (članak 114. UFEU-a, koji se odnosi na usklađivanje unutarnjeg tržišta), ta iznimka ne bi uključivala predloženi EU-ov centar.

procijeni te zahtjeve i EU-ovu centru proslijedi osobne podatke samo ako je to strogo nužno i razmjerno potrebnoj svrsi.

Članak 10. stavak 6. o ulozi Europolu u obavješćivanju korisnika nakon provedbe naloga za otkrivanje

134. EDPB i EDPS pozdravljaju zahtjev, kako je utvrđen u članku 10. stavku 6. Prijedloga, da pružatelji usluga obavijeste korisnike osobnih podataka na koje bi se izvršenje naloga za otkrivanje moglo odnositi. Te bi se informacije korisnicima trebale pružiti tek nakon dobivanja potvrde Europolu ili nacionalnog tijela za izvršavanje zakonodavstva države članice koje je primilo prijavu u skladu s člankom 48. Prijedloga da pružanje informacija korisnicima neće ometati aktivnosti za sprečavanje, otkrivanje, istragu i progon kaznenih djela seksualnog zlostavljanja djece.
135. Međutim, praktična provedba te odredbe nije konkretno navedena. Kad se prijave prosljeđuju Europolu i tijelu za izvršavanje zakonodavstva države članice, u Prijedlogu se na navodi je li potrebna potvrda jednog ili obaju primatelja niti su u Prijedlogu navedeni postupci/modaliteti za dobivanje te potvrde (npr. treba li potvrde uputiti preko EU-ova centra). Uzimajući u obzir veliku količinu materijala koji sadržava seksualno zlostavljanje djece koju bi Europol i nacionalna tijela za izvršavanje zakonodavstva trebali obraditi te nepostojanje točnog roka za dostavljanje potvrde („bez nepotrebne odgode”), EDPB i EDPS preporučuju da se pojasne primjenjivi postupci kako bi se osigurala realizacija te zaštitne mjere u praksi. Nadalje, obveza obavješćivanja korisnika trebala bi uključivati i informaciju o primateljima predmetnih osobnih podataka.

O prikupljanju podataka i izvješćivanju radi transparentnosti (članak 83.)

136. Člankom 83. stavkom 3. Prijedloga predviđa se da EU-ov centar prikuplja podatke i izrađuje statističke podatke koji se odnose na niz njegovih zadaća na temelju predložene uredbe. Za potrebe praćenja, EDPB i EDPS preporučuju da se na taj popis dodaju statistički podatci o broju prijavi prosljeđenih Europolu u skladu s člankom 48. te o broju zahtjeva za pristup koje je Europol primio na temelju članka 46. stavaka 4. i 5., uključujući broj zahtjeva koje je EU-ov centar odobrio i odbio.

5. ZAKLJUČAK

137. Iako EDPB i EDPS pozdravljaju nastojanja Komisije da se osigura učinkovito djelovanje protiv seksualnog zlostavljanja djece na internetu, smatraju da Prijedlog izaziva ozbiljnu zabrinutost u pogledu zaštite podataka i privatnosti. Stoga EDPB i EDPS pozivaju suzakonodavce da izmijene predloženu uredbu, osobito kako bi se osiguralo da predviđene obveze otkrivanja ispunjavaju primjenjive standarde nužnosti i proporcionalnosti te da ne dovode do slabljenja šifriranja na općoj razini. EDPB i EDPS i dalje su na raspolaganju za pružanje potpore tijekom zakonodavnog postupka ako se smatra da je njihov doprinos potreban za rješavanje pitanja istaknutih u ovom zajedničkom mišljenju.

Za Europskog nadzornika za zaštitu podataka

Za Europski odbor za zaštitu podataka

Europski nadzornik za zaštitu podataka

Predsjednica

(Wojciech Wiewiorowski)

(Andrea Jelinek)